A CRYPTOGRAPHIC SERIES

REVISED EDITION

59

CRYPTANALYSIS
OF THE
SINGLE COLUMNAR TRANSPOSITION CIPHER

INCLUDES COMPUTER PROGRAM WRITTEN IN BASIC

Numerical Key

1	2	3	4	5	6	7	8	9	10
			J	L	E	E			
		O	R	N	D	E			
	U	D	O	T	G	E			
E	F	E	O	P	R	E	S	O	L
I	S	E	S	L	F	S	N	N	E
P	S	R	C	H	T	A	U	P	L
E	E	T	L	E	E	O	L	T	I
I	T	J	N	D	E	I	P	A	V
E	O	R	T	G	E	T	V	D	L
U	D	O	P	R	E	S	O	A	T

By

Wayne G. Barker

From Aegean Park Press

BAR
1992

005.82 BAR 1992
Barker, Wayne G.
Cryptanalysis of the single column
OBC01 OB1 C.1
23694-10

מועד להחזרה

21/03/99			
21.04.99			

CRYPTANALYSIS
OF
THE SINGLE COLUMNAR TRANSPOSITION
CIPHER

Cryptanalysis

of

The Single Columnar Transposition Cipher

by

Wayne G. Barker

99-567
23694-10
לת אורט בראודה
ספריה
קרית המכללה ת.ד. 78 כרמיאל 20101
מס' פריט 23694-01
' מיון 00582
BAR

© 1992 by AEGEAN PARK PRESS

The original edition of *Cryptanalysis of the Single Columnar Transposition Cipher* was published in 1961 by the Charles E. Tuttle Company, Rutland, VT, and Tokyo, Japan. Copyright in Japan, 1961, the original edition contained the Library of Congress Catalog Card No. 61-11556.

The present revised edition of *Cryptanalysis of the Single Columnar Transposition Cipher* contains a rewritten Chapter XVI, an added Chapter XVII, which contains material concerning the application of the computer to the cryptanalysis of the single columnar transposition cipher, and a computer program, written in BASICA, that provides for computer encipherment of the single columnar transposition cipher.

ISBN: 0-89412-192-8 (soft cover)
ISBN: 0-89412-193-6 (library bound)

AEGEAN PARK PRESS
P.O. Box 2837
Laguna Hills, California 92654
(714) 586-8811
FAX (714) 586-8269

Manufactured in the United States of America

PREFACE

This book *Cryptanalysis of the Single Columnar Transposition Cipher* is a text-book. It presents to the student cryptanalyst a comprehensive course of study covering the single columnar transposition cipher system. In line with its being a text-book, at the end of each chapter are either a series of questions or a number of problems covering the particular material or "points" presented within the chapter. The author feels that the problems in particular give a tremendous asset to the book. For not only will the problems provide many dozens of hours of enjoyment, but in the final analysis the problems will be the best actual teaching aid of the book.

Some idea of the broad scope of the text which covers almost every conceivable aspect of the single columnar transposition cipher is the following: Chapter I opens the text by showing exactly where the single columnar transposition cipher system fits into the large family of cryptographic systems. The next two chapters cover *encipherment* and *decipherment* respectively. The next several chapters cover certain background cryptanalytic techniques and procedures which are necessary in the cryptanalytic solution of the single columnar transposition cipher. It is not until Chapter VII in fact that the cryptanalytic problem of the single columnar transposition cipher is finally discussed. By this time the student is well prepared! Beginning with Chapter VII cryptanalytic problems and techniques are presented in almost minute detail. Each successive chapter uses as background previously presented material, and the text finally builds up to the *general cryptanalytic solution* of the single columnar transposition cipher, found in the next to last chapter, Chapter XV. The last chapter then wraps up the text with "final remarks". At this point, the student should indeed be proficient when it comes to the analytic solution of the single columnar transposition cipher system — particularly if he has conscientiously done the problems!

Of course it should be realized too that after completing the book the student not only will "know" the single columnar transposition cipher, but he also will have a fine background foundation for the study of other transposition cipher systems whose solutions involve similar techniques and procedures.

Finally, the author deems it only proper to state that probably certain inadvertent errors will have "crept" into the text, in spite of many hours checking, and double checking! These errors he hopes are few. None have been made on purpose.

With respect to the problems, all do have a solution.

Good-luck!

WGB

TABLE OF CONTENTS

PAGE

PREFACE v
LIST OF FIGURES ix

CHAPTER I. THE FAMILY TREE 1
Questions 1–5 3

CHAPTER II. THE KEY 4
Questions 1–10 7

CHAPTER III. ENCIPHERMENT 8
Questions 1–12 11

CHAPTER IV. DECIPHERMENT 12
Questions 1–10 16

CHAPTER V. THE MONOLITERAL FREQUENCY DISTRIBUTION 17
Questions 1–10 23

CHAPTER VI. THE BILITERAL FREQUENCY DISTRIBUTION 24
Questions 1–7 28

CHAPTER VII. INTRODUCTION TO CRYPTANALYSIS GIVEN: THE PLAIN-TEXT BEGINNING OF A MESSAGE LONGER THAN THE KEY-LENGTH 29
Problems 1–10 35

CHAPTER VIII. THE ANALYTIC MATRIX 37
Questions 1–8 43

CHAPTER IX. CRYPTANALYTIC SOLUTION GIVEN: PLAIN-TEXT LONGER THAN THE KEY-LENGTH ANYWHERE IN THE MESSAGE 44
Problems 11–20 50

CHAPTER X. CRYPTANALYTIC SOLUTION GIVEN: THE KEY-LENGTH AND A COMPLETELY FILLED MATRIX 52
Problems 21–30 60

CHAPTER XI. IDENTIFICATION OF THE "COMPLETELY FILLED MATRIX" 62
Problems 31–40 77

CHAPTER XII. CRYPTANALYTIC SOLUTION GIVEN: THE KEY-LENGTH PLUS A PROBABLE WORD IN THE TEXT 79
Problems 41–50 89

CHAPTER XIII. CRYPTANALYTIC SOLUTION GIVEN: A PROBABLE WORD IN THE TEXT 91
Problems 51–60 104

CHAPTER XIV. CRYPTANALYTIC SOLUTION GIVEN: THE KEY-LENGTH 106
Problems 61–70 115

CHAPTER XV. CRYPTANALYTIC SOLUTION THE GENERAL SOLUTION 117
Problems 71–80 128

CHAPTER XVI. FINAL REMARKS 130
Problems 81–90 133

CHAPTER XVII. THE COMPUTER 135
Problems 91–100 139

GENERAL INDEX 141

LIST OF FIGURES

PAGE

Figure 1. The Family Tree 2

Figure 2. Expected Frequency of Letters in English 19

Figure 3. Letter Contact Weight Chart 55

Figure 4. Table of Key-Lengths and Column-Lengths of Completely Filled Matrices—Given the Message-Length ... 70

Figure 5. The 100 Most Frequent Trigraphs 108

CRYPTANALYSIS
OF
THE SINGLE COLUMNAR TRANSPOSITION
CIPHER

Chapter I

The Family Tree

In general all cryptographic systems may be divided into two large and distinct classes—*code systems* and *cipher systems.*

A *code* is a cryptographic system in which varying lengths of plain-text, usually words or complete phrases, are replaced by *code groups.* The *key* in a code system is the *code book* wherein are found the code groups. Since relatively short code groups replace words or phrases, a code may be used for the purpose of obtaining brevity as well as for obtaining security.

A *cipher,* on the other hand, is a cryptographic system in which fixed lengths of plain-text, usually single letters or pairs of letters, are treated in such a way as to make the resulting cipher-text unintelligible without the key. The key in a cipher system often is a word, this word being termed the *key-word.*

The treatment of the plain-text in a cipher system normally takes one of two forms; though a combination of both forms is possible. These two forms are:

(1) In the case of a *substitution cipher,* as the term denotes, a substitution takes place. That is, other letters, digits, or even symbols, are substituted for the plain-text letters being enciphered. For example, if in a particular cipher system, the letters of the word THE are replaced by the letters UIF, a substitution has taken place and this therefore is a substitution cipher system.

(2) In the case of a *transposition cipher,* again as the term denotes, a transposition takes place. That is, the plain-text letters being enciphered are rearranged or transposed, the rearrangement or transposition being the cipher-text. For example, if the letters of the word LAUGH are transposed as HLGUA, a transposition (rather than a substitution) has taken place and this then is a transposition cipher system—provided of course that the transposition has followed a plan or system as agreed upon between correspondents.

Within both the *substitution cipher* and the *transposition cipher* there are many hundreds of specific systems, and when combinations of these many systems are considered there is almost a limitless number. This book deals with but one of these specific cryptographic systems, one which is in the transposition cipher family, the *single columnar transposition cipher.*

Figure 1 shows graphically where the *single columnar transposition cipher* fits in the family tree of cryptographic systems which we have just discussed.

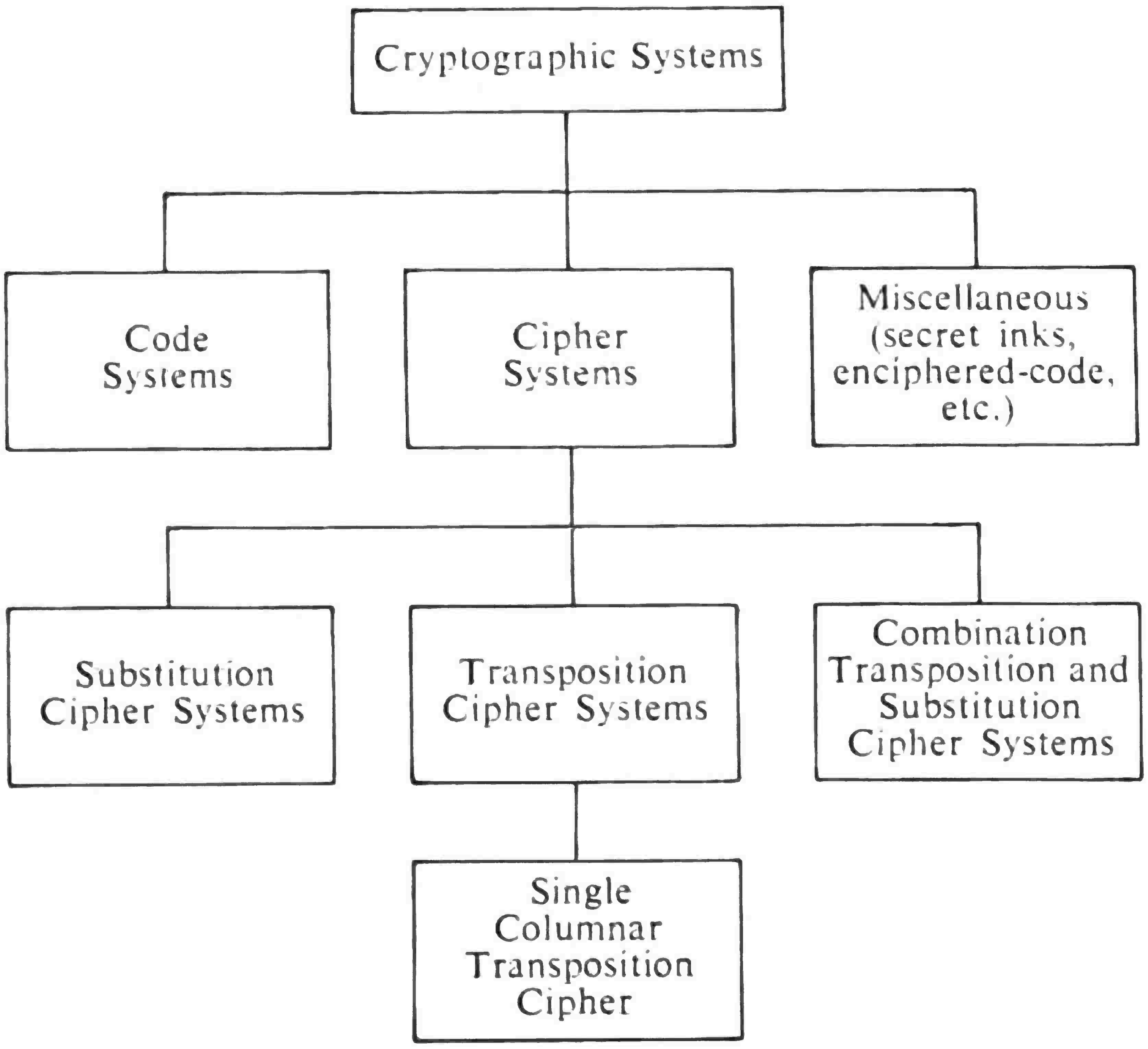

Cryptographic Systems
Code Systems
Cipher Systems
Miscellaneous (secret inks, enciphered-code, etc.)
Substitution Cipher Systems
Transposition Cipher Systems
Combination Transposition and Substitution Cipher Systems
Single Columnar Transposition Cipher

FIGURE 1.

Questions

1. Generally speaking all cryptographic systems are divided into two large classes. What are these two classes?

2. What is the key in the case of a code system?

3. Cipher systems may be divided into two general types. What are these two types?

4. The plain-text word AND is enciphered in a particular cipher system. The resulting cipher-text equivalent to the word AND are the letters ZMC. Is this particular cipher system of the transposition type or the substitution type? How can you tell?

5. The plain-text message NO REPLY RECEIVED TO MY LETTER OF THE FIRST is enciphered in a particular cipher system. The resulting cipher-text message is:

   ```
   RRVMT TRNLE TEOFP CDLRE TOYIO
   TFIEE EYEHS
   ```

   Is this a transposition or substitution cipher system? Why?

Chapter II

The Key

In order to encipher or to decipher messages using the single columnar transposition cipher system, correspondents or users need but one thing, the *key*. The key in a cipher system is that secret element, often a secret *key-word,* knowledge of which allows a message to be enciphered or deciphered. In the case of the single columnar transposition cipher system this key takes the form of a *numerical key,* that is, a keyed mixed series of numbers. For example, a numerical key might be: 5 8 4 7 2 1 6 3. This particular key has a key-length of eight. That is, there are eight different numbers or digits in the key. Note that the digits 1 through 8 occur in mixed order within the key.

It can easily be seen that it would be difficult for correspondents to remember or to memorize a series of mixed numbers comprising a numerical key. Therefore, in the normal use of the single columnar transposition cipher, the correspondents, instead of memorizing a numerical key, merely remember a *literal key* or key-word. From this more easily remembered literal key the desired numerical key is then derived. Let us see now how this derivation is accomplished.

There are various methods by which a numerical key may be derived from a literal key. The most common method perhaps and the method which will be used in this book is the following:

Consider the literal key to be the key-word SUITCASE. From this literal key we desire to derive a numerical key.

The key-word is written horizontally as follows:

S U I T C A S E

Beneath the letters of this key-word are written the digits of the numerical key. To begin, in the key-word SUITCASE the letter nearest the top of the alphabet is the letter A. Therefore, beneath the letter A is written the digit 1:

S	U	I	T	C	A	S	E
					1		

Going down the alphabet, the next letter to appear in the key-word is the letter C. Therefore, beneath the letter C is written the digit 2:

S	U	I	T	C	A	S	E
				2	1		

Similarly, the next letter to appear in the key-word is the letter E. Hence, beneath the letter E is placed the digit 3:

S	U	I	T	C	A	S	E
				2	1		3

The next letter is I. Therefore beneath the I is placed a 4:

S	U	I	T	C	A	S	E
		4		2	1		3

The next letter is S. But in this case there are two letter S's. What do we do when repeated letters occur in the key-word? The answer is simple. Beneath the repeated letter nearest to the left is placed the next digit, in this case 5, and going then towards the right, beneath the next common or repeated letter is placed the next successive digit, in this case 6. We then have:

S	U	I	T	C	A	S	E
5		4		2	1	6	3

Beneath the next letter T is placed a 7, and finally beneath the last letter U is placed the digit 8. The final result is:

S	U	I	T	C	A	S	E
5	8	4	7	2	1	6	3

Thus, the numerical key resulting from or derived from the key-word SUITCASE is: 5 8 4 7 2 1 6 3.

One point might be made regarding the numerical key as derived from a literal key. A literal key will result in only one specific numerical key—provided of course that the same method of derivation is followed each time. However, *the same numerical key may result from two or more different literal keys.* For example, the numerical key 5 3 1 2 4 6 results from the literal key SLEEPY as well as from the literal key NICELY.

In the next chapter we shall see how the numerical key, as derived from a literal key, is used to encipher a message in the single columnar transposition cipher system.

Questions

1. In the single columnar transposition cipher system is the literal key derived from the numerical key? Or vice-versa?
2. Is it easier for a correspondent to remember a literal key or a numerical key?
3. If a numerical key is derived from a key-word of 12 letters, what will the length be of the numerical key?
4. If a key-word contains a repeated letter, beneath which of the repeated or common letters is placed the smaller digit?
5. What is the numerical key derived from the the key-word STEAMBOAT?
6. The key-word WINTER TIME results in what numerical key?
7. What is the numerical key resulting from the key-word HARD LUCK?
8. May the same numerical key be obtained from two or more different key-words?
9. Is it possible to employ the single columnar transposition cipher system using numerical keys *not* derived from literal keys?
10. Why is it normally desirous to use literal key-words instead of random numerical keys?

Chapter III

Encipherment

Perhaps the best manner in which to describe the enciphering process of the single columnar transposition cipher system is to go through the steps in the encipherment of an actual message. Therefore, let us be given the following:

Message: NEED SUPPLIES AT ONCE STOP REQUEST
REPLY IMMEDIATELY

Literal key: SUMMER TIME

Our *first step* is to obtain the necessary numerical key from the given literal key, in this case the words SUMMER TIME. Using the procedure learned in Chapter II we easily arrive at the following:

S U M M E R T I M E
8 10 4 5 1 7 9 3 6 2

The *second step* in the enciphering process is to write the text of the plain-text message beneath the numerical key as follows:

S	U	M	M	E	R	T	I	M	E
8	10	4	5	1	7	9	3	6	2
N	E	E	D	S	U	P	P	L	I
E	S	A	T	O	N	C	E	S	T
O	P	R	E	Q	U	E	S	T	R
E	P	L	Y	I	M	M	E	D	I
A	T	E	L	Y					

Note that the message when written beneath the numerical key forms what might be termed an incomplete square. This square in cryptographic terminology is called a *matrix*. There are two kinds or types of matrices, the *completely filled matrix* and the *in-completely filled matrix*. In the completely filled matrix the bottom or last line of the matrix extends completely across the bottom of the matrix, making a complete square. Putting it another way, in the completely filled matrix the length of the message (in number of letters) is a multiple of the key-length! In the example above, the matrix is an in-completely filled matrix.

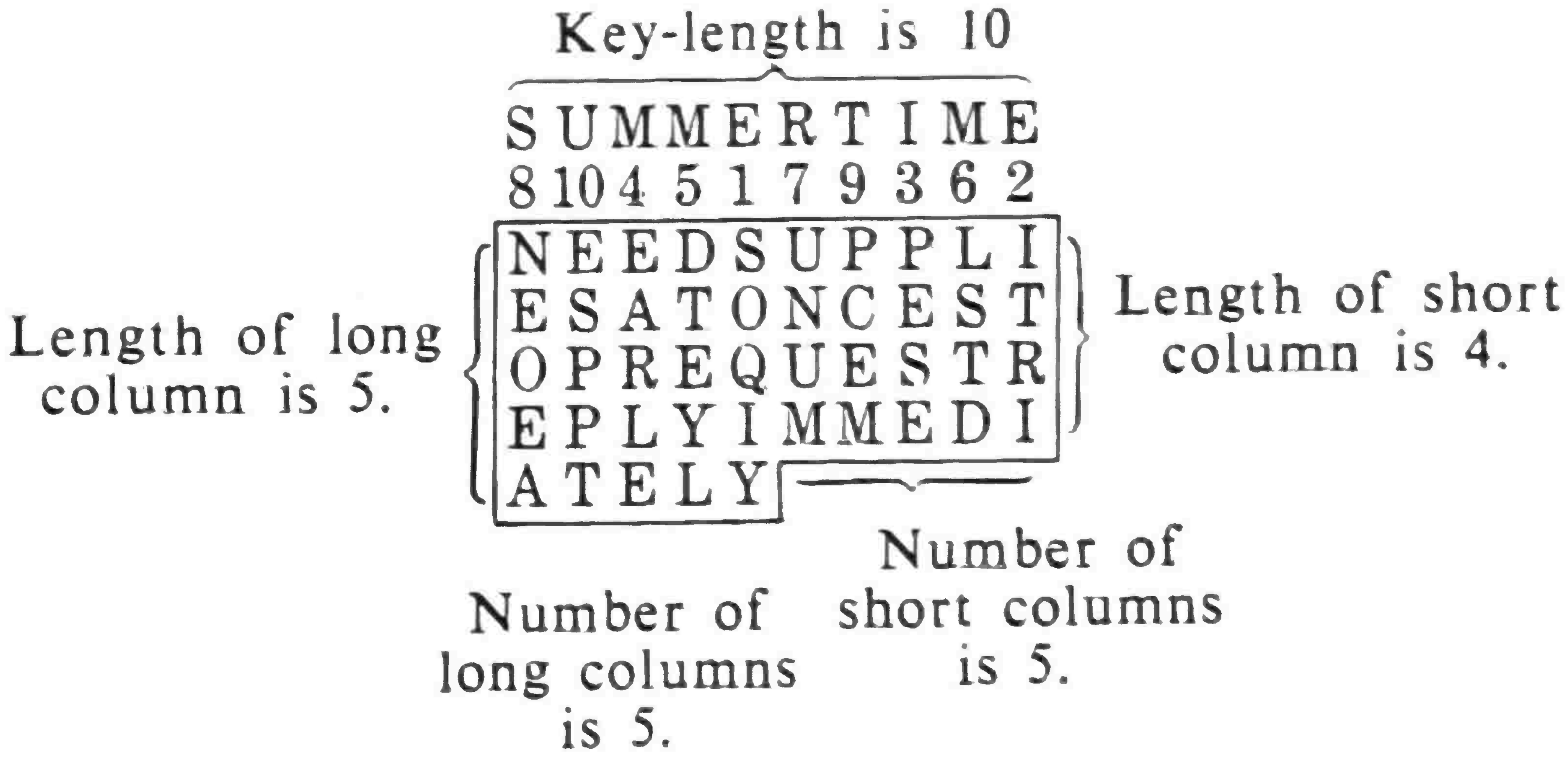
The size or dimensions of any matrix depends upon two things:

(1) The length of the key.

(2) The length of the message.

That is, given these two things, we can determine whether the matrix is completely or in-completely filled. We can also determine the length of the columns in the matrix, the number of long columns in the matrix, the number of short columns in the matrix, etc.

In order to make these terms clearer, in the example above note that there are ten columns in the matrix. Thus, there is one column for each letter or digit of the key. Note also that the length of a short column is four, the length of a long column is five, the number of long columns is five, and the number of short columns is five. Graphically, these may be shown as follows:



Key-length is 10
Length of long column is 5.
Length of short column is 4.
Number of short columns is 5.
Number of long columns is 5.

S	U	M	M	E	R	T	I	M	E
8	10	4	5	1	7	9	3	6	2
N	E	E	D	S	U	P	P	L	I
E	S	A	T	O	N	C	E	S	T
O	P	R	E	Q	U	E	S	T	R
E	P	L	Y	I	M	M	E	D	I
A	T	E	L	Y					

Returning to our encipherment process, having written the message on successive lines beneath the numerical key, our *third step* in enciphering is to take the columns out of the matrix in numerical order. Thus, the first column to be taken out of the matrix is column 1 or S O Q I Y. This column of letters forms the beginning of the cipher-text message or *cryptogram*. The second column is I T R I. These four letters follow the first five in the cipher-text message. Column 3 follows column 2, and so on, until finally column 10 is reached or taken out; and the cipher-text message appears as follows:

SOQIYITRIPESEEARLEDTEYLLS
TDUNUMNEOEAPCEMESPPT

Since cryptographic text is normally divided into so-called "code" groups, we divide the message into five letter groups, and the final enciphered message is as follows:

SOQIY ITRIP ESEEA RLEDT EYLLS
TDUNU MNEOE APCEM ESPPT

Note that the letters of the original plain-text message have not been changed. They have been merely re-arranged or transposed. Remember also that the "key" to this transposition of letters was a numerical key—derived from an easily remembered literal key-word.

Questions

1. In order to encipher a message using the single columnar transposition cipher system, only one thing or element is needed. What is this one element?
2. What is the *first step* of encipherment?
3. What is the *second step* of encipherment?
4. What is the *third step* of encipherment?
5. What are the two possible kinds of matrices?
6. If the message length is a multiple of the key-length, what kind of a matrix will result?
7. The dimensions of a matrix depends upon two things. What are these two things?
8. The number of columns in a matrix depends upon what?
9. If there is but one common column length in a particular matrix, what kind of a matrix is it?
10. The order in which columns are taken out of the matrix depends upon what?
11. Using the key-word BROKER, encipher the message: SEND BAGGAGE TO SAN FRANCISCO IMMEDIATELY.
12. Encipher the message of Question 11 using the key-word: SOAP SUDS.

Chapter IV

Decipherment

Now that we have learned in Chapter III how to encipher a message, let us consider the decipherment of a message. In general, the process of decipherment is the reverse of encipherment. Consider the decipherment of the following message:

```
UNCKO  MNHTA  NSEOT  NMIEG  OFPER
NMAWO  OLTGA  SFHDO  OLLEN  YINRI
SIECY  COTOR  FETNN  TSGOR  IPTHT
NOETX  ISENW  ICXMI  NREUE  T
```

Key-word: APPLE BLOSSOMS

Just as in encipherment, our *first step* is to derive a numerical key from the literal key:

```
A P P  L E B L O S  S  O M S
1 9 10 4 3 2 5 7 11 12 8 6 13
```

The *second step* in decipherment is to determine the size of the matrix used in encipherment. This is perhaps the major crux of decipherment. We know the length of the key. In the key above the length is 13. We also can count the number of letters in the cipher-text message. In the above case, there are 96 letters in the cipher-text message. Thus, we have the two requirements to determine the dimensions of the matrix, the key-length and the message length.[1] Dividing the key-length into the message length yields the following:

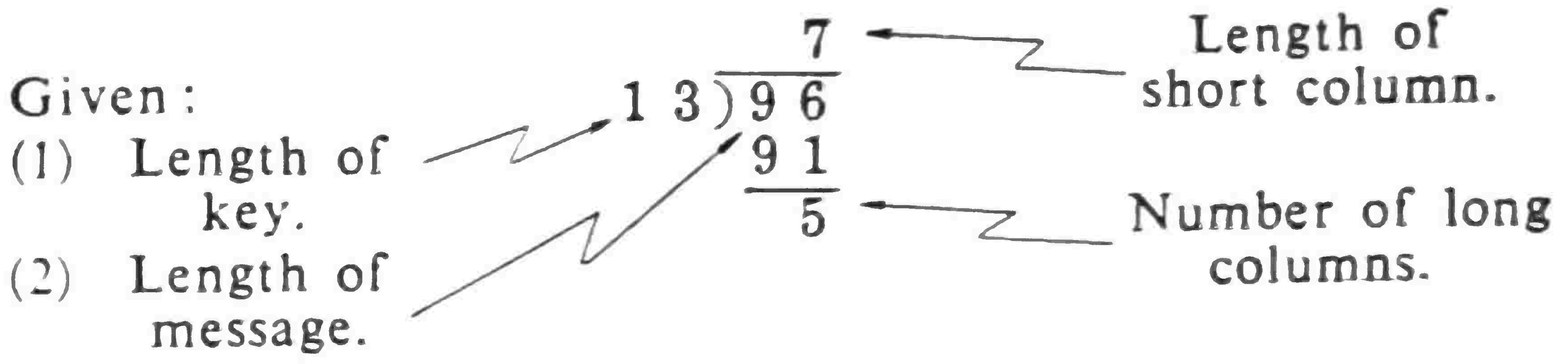
$$\begin{array}{r} 7 \\ 13\overline{)96} \\ \underline{91} \\ 5 \end{array}$$

---

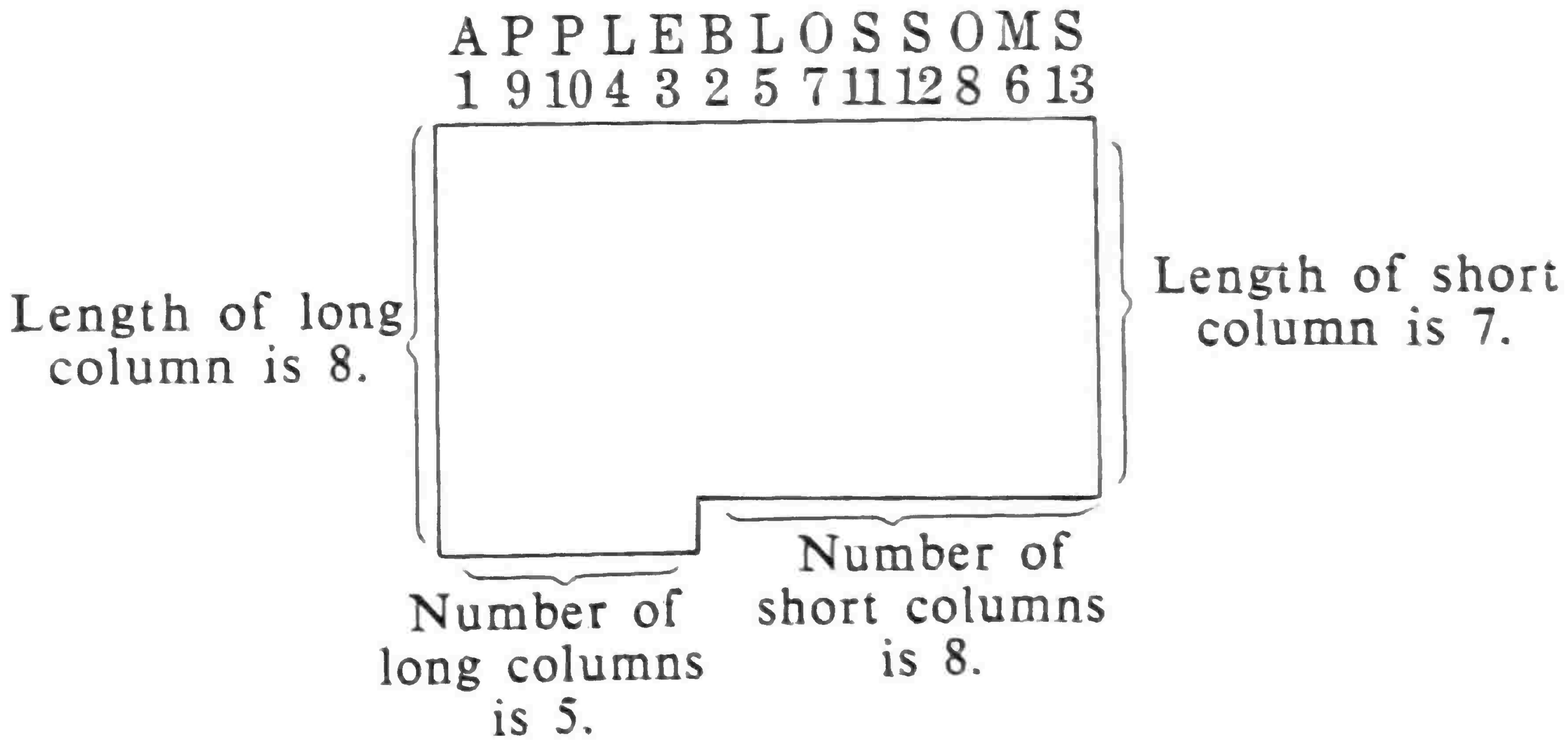
[1] See page 9.

The number of times that the key-length (13) goes into the message length (96) is the *length of a short column* in the matrix, in this case 7. The left over remainder, in this case 5, is the *number of long columns* in the matrix.

Let's take another look at this division, since it is so fundamental:



Since the length of a short column is 7, the *length of a long column* is one more, or 8. And too, since the number of long columns is 5, the *number of short columns* is the key-length minus the number of long columns (13-5) or 8. Thus, in the present case, given the key and the cipher-text message, we have determined the size of the matrix used in encipherment to be the following:


A P P L E B L O S S O M S
1 9 10 4 3 2 5 7 11 12 8 6 13
Length of long column is 8.
Length of short column is 7.
Number of long columns is 5.
Number of short columns is 8.

Now that we know the lengths of the various columns it is fairly easy to proceed to the *third step* of decipherment, putting the columns from the cipher-text message back into the matrix according to the numerical key. Thus, looking at the empty matrix above we see that column 1 is a long column of length 8. Therefore, the first eight letters of the cipher-text message go into column 1:

A	P	P	L	E	B	L	O	S	S	O	M	S
1	9	10	4	3	2	5	7	11	12	8	6	13
U												
N												
C												
K												
O												
M												
N												
H												

Column 2 is a short column of length 7. Therefore, the next seven letters of the cipher-text message go into column 2:

A	P	P	L	E	B	L	O	S	S	O	M	S
1	9	10	4	3	2	5	7	11	12	8	6	13
U					T							
N					A							
C					N							
K					S							
O					E							
M					O							
N					T							
H												

Column 3 is a long column. Therefore, the next eight letters from the cipher-text message go into column 3. In a similar manner, the remaining letters are put into the matrix in column order. After the last seven letters of the cipher-text are put into column 13, the now filled matrix looks as follows:

A	P	P	L	E	B	L	O	S	S	O	M	S
1	9	10	4	3	2	5	7	11	12	8	6	13
U	R	G	E	N	T	L	Y	N	E	E	D	I
N	F	O	R	M	A	T	I	O	N	C	O	N
C	E	R	N	I	N	G	N	E	W	Y	O	R
K	T	I	M	E	S	A	R	T	I	C	L	E
O	N	P	A	G	E	S	I	X	C	O	L	U
M	N	T	W	O	O	F	S	I	X	T	E	E
N	T	H	O	F	T	H	I	S	M	O	N	T
H	S	T	O	P								

The plain-text or clear-text message may now be read horizontally from left to right, top to bottom within the matrix. There may be perhaps a slight difficulty in reading the plain-text words, since as can be seen there is no spacing between words. However, with a little practice this difficulty is easily overcome. The complete plain-text message reads:

> URGENTLY NEED INFORMATION CONCERNING
> NEW YORK TIMES ARTICLE ON PAGE SIX COL-
> UMN TWO OF SIXTEENTH OF THIS MONTH STOP

Now that we have gone through the steps in the decipherment of a cipher-text message, in order to thoroughly keep the steps in mind, let us briefly compare the steps of encipherment with the steps of decipherment:

STEPS	ENCIPHERMENT	DECIPHERMENT
1st	Derive the numerical key from the literal key-word	Derive the numerical key from the literal key-word
2nd	Write the plain-text beneath the numerical key	Determine size of matrix from key-length and message length
3rd	Take columns *out* of matrix in numerical order	Put columns *into* matrix in numerical order

One final remark is in order concerning the determination of the size of the matrix, given the key-length and the message length. There is another way, other than that described, of determining the length of matrix columns. It is simply a mechanical method whereby after the numerical key is written down, a number of squares are counted beneath the key equal to the length of the message. The size of the matrix is thus manually or physically determined without recourse to any actual mathematical computation.

Questions

1. Is the *first step* of decipherment different from the *first step* of encipherment?

2. What is the *second step* of decipherment?

3. What is the *third step* of decipherment?

4. If the key-length is 12 and the length of a message is 83 letters, what is the length of the short column in the matrix? How many short columns are there?

5. If the key-length is 7 and the message length is 92 letters, how many long columns are there? What is the length of the long column?

6. With the key-word GEORGIA TECH read the following message:

   IBXRF TNCYU EIMYB TANGA TRSRT
   ONOAI XTRAO IRRTT NXSEN TAXEH
   TULXR ELOIM EOA

7. With the key-word ORANGES read the following message:

   RAEON ESSUE LDESS WLTAU OWRTE
   FDOER HKGGT ROE

8. With the key-word STICKY read the following message:

   RMGDN KEYNE ECYGE CFOTE NTLRL
   DMCIL TOAEE AOCO

9. With the key-word TAXICABS read the following message:

   EEIIP UEUAR NTSAN MSOIQ WOONK
   DSFNE CRTAH FLHTS TIQVA RNOMI
   R

10. With the key-word LEMON CAKE read the following message:

    OSEMT ERFHU BEELH YROTA SMDEO
    SENSB OOETF D

Chapter V

The Monoliteral Frequency Distribution

One of the fundamental tools of the cryptanalyst is the *frequency distribution.* Whether the cryptanalyst is attempting to solve one type of cryptographic system or another, almost invariably the frequency distribution will play a prominent role in solution. The reason for this is that in normal plain-text various letters will "in the long run" occur with a definite frequency of occurrence. Thus, for example, in normal English plain-text the letter E occurs more frequently than any other letter. Cryptanalysts who have made thousands of tabulations, counting plain-text letters, know down to a very fine point the exact "expected frequency" of each letter. A frequency distribution of individual letters is known as a *monoliteral frequency distribution.*

Consider the following cryptogram:

HEHBL LRNFN TYSED FOACS HAHTA
ETGUL TOIRR ETAES IEEYP SIEPM
TSMHF NBEES NITOI LESPN POSCI
SOTAA RPROS TNTSL IUAFI

A monoliteral frequency distribution of this message is made as follows: The normal alphabet is written out and the occurrence of the letters in the cryptogram or cipher-text message are then tabulated beneath the letters of this alphabet. To begin, the first letter of the above cryptogram is H. Therefore, beneath the letter H of the alphabet is made a mark or tabulation:

A B C D E F G $\underline{\text{H}}$ I J K L M N O P Q R S T U V W X Y Z

The next letter of the message is E. Therefore, in the same manner beneath the letter E is made a mark:

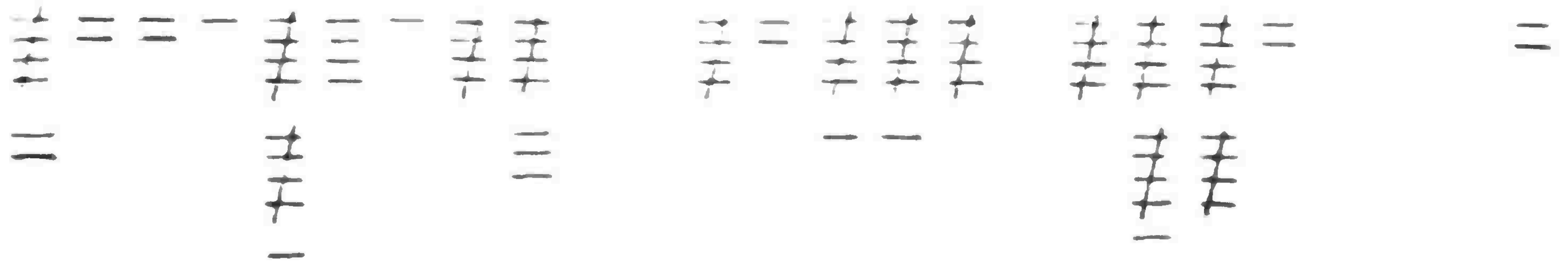
A B C D $\underline{\text{E}}$ F G $\underline{\text{H}}$ I J K L M N O P Q R S T U V W X Y Z

Continuing, the third letter is another H. Hence, again beneath the letter H is made another mark:

A B C D $\underline{E}$ F G $\underline{\underline{H}}$ I J K L M N O P Q R S T U V W X Y Z

Successive marks or tabulations are made until all occurrences of each letter are marked beneath their respective letters. The final completed monoliteral frequency distribution then looks as follows:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z



Note that every fifth mark beneath a letter is made in the form of a diagonal crossing the preceding four marks. This is merely to aid in the later counting of the total number of marks beneath letters. It should be realized also that this frequency distribution could just as well have been made vertically as follows:

A	𝍸 𝍷𝍷
B	𝍷𝍷
C	𝍷𝍷
D	𝍷
E	𝍸 𝍸 𝍷
F	𝍷𝍷𝍷𝍷
G	𝍷
H	𝍸
I	𝍸 𝍷𝍷𝍷
J	
K	
L	𝍸
M	𝍷𝍷
N	𝍸 𝍷
O	𝍸 𝍷
P	𝍸
Q	
R	𝍸
S	𝍸 𝍸 𝍷
T	𝍸 𝍸
U	𝍷𝍷
V	
W	
X	
Y	𝍷𝍷
Z	

Now that a monoliteral frequency distribution has been made of this particular message, what purpose does the distribution serve? Essentially of course the distribution shows the number of times each letter has occurred in the message. One thing the distribution as a whole can do is to indicate whether or not the cryptogram is of the transposition type or class, as opposed to the substitution. As you recall from Chapter I, in the transposition cipher system there is a rearrangement or transposition of plain-text letters, such that *the final resulting cipher-text still contains exactly the same letters as did the original plain-text,* except now in a different order. Thus, for example, the monoliteral frequency distribution above indicates that the letter E has occurred 11 times. In the original plain-text message the letter E must have occurred the same number or 11 times—provided of course that the cipher system employed is of the transposition type.

Therefore, by comparing the monoliteral frequency distribution of the message with the normal or expected monoliteral frequency distribution of English plain-text, we can with relative accuracy determine whether or not the message has been enciphered by means of a transposition cipher system.

The normal expected frequency of English letters in 100 letters of text is the following:

Expected Frequency of English Letters
in 100 Letters of Text

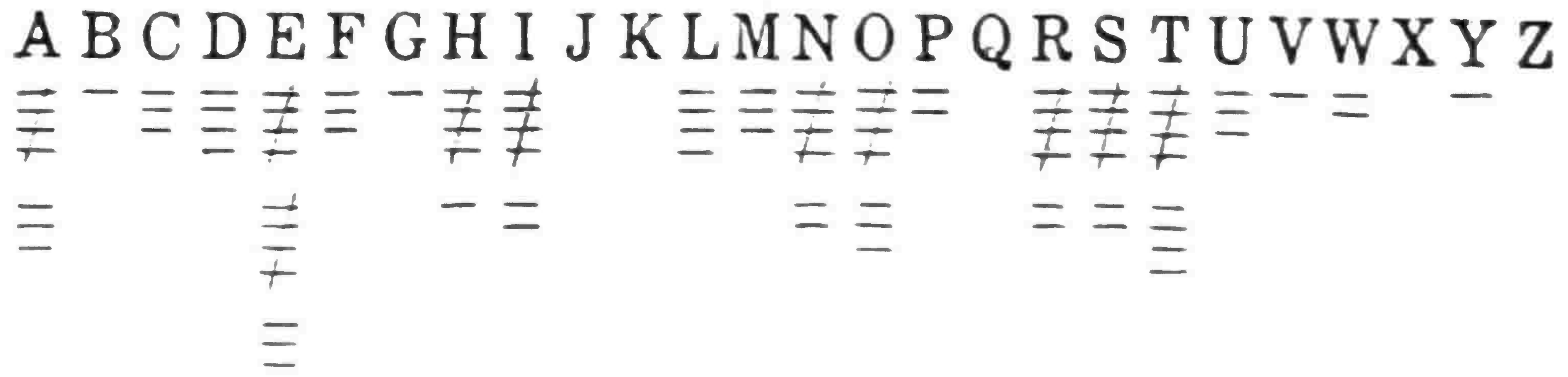
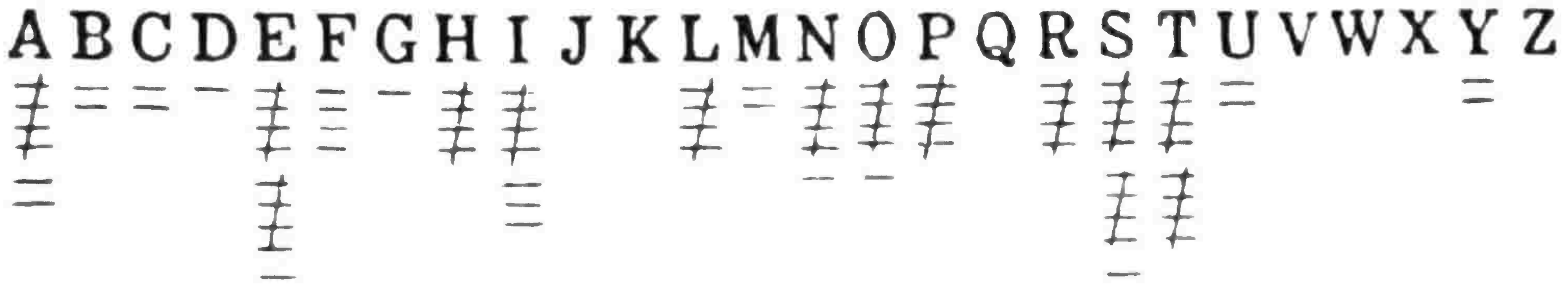


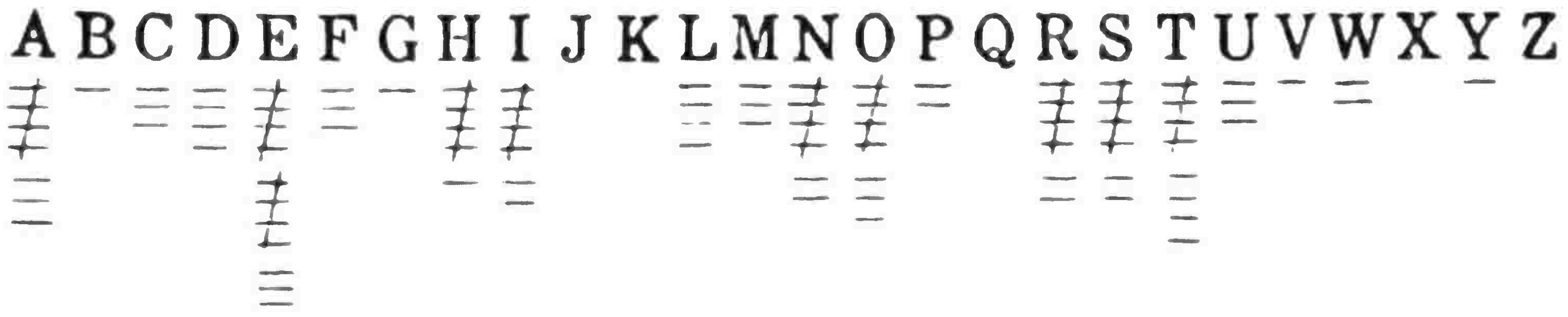
FIGURE 2

Let us compare the distribution of Figure 2 which is the *norm* for English text with the monoliteral frequency distribution previously made from the cipher-text of the given message:

Cryptogram:



The *norm*:

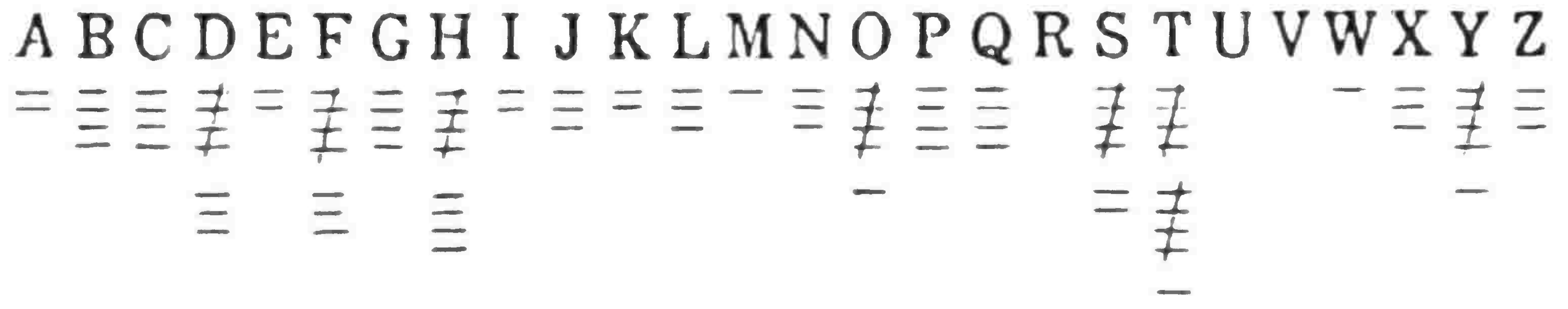


It is easily seen that the two distributions are remarkably similar, *particularly when the "troughs and peaks" of the two distributions are compared!* This comparison indicates that almost certainly the given cryptogram or cipher-text message is of the transposition type.

Consider now the monoliteral frequency distribution of a cryptogram which is *not* of the transposition type:

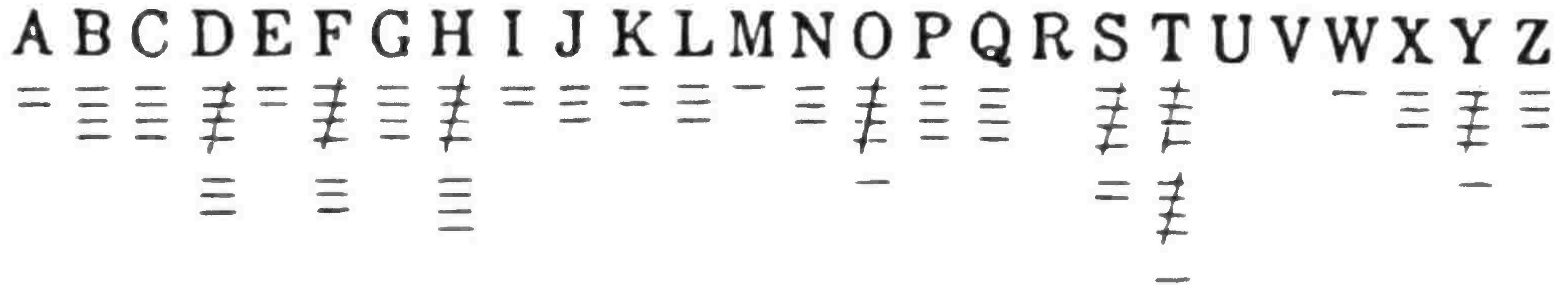
JCTDT BSDHC GBSAK OTBQP FNSOH
BSWFZ HCFOT DGXFL TDKLG OTNGD
TYIOH YTNQP FLJDT YHAFP FMQEH
ESDTC TDHPS YHXQZ FYJXI OHYSZ

Monoliteral Frequency Distribution:

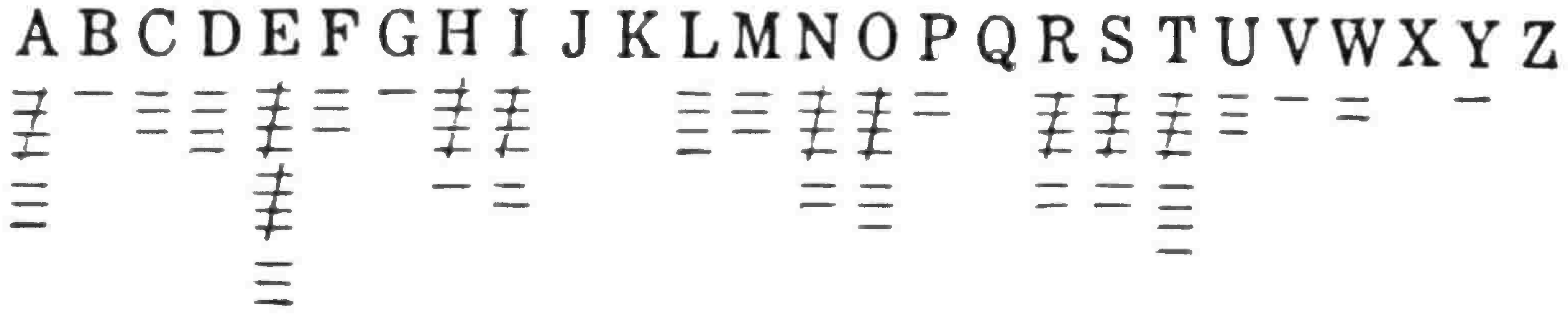


Let us compare this frequency distribution with the *norm* for English text:

Cryptogram:



The *norm*:



In this case it is seen that the two distributions are not similar. In other words, it is evident that this second cryptogram is not of the transposition type.

A few comments are in order regarding the identification of a transposition cipher by use of the monoliteral frequency distribution. In the English language the vowels (A, E, I, O, U, and Y) constitute fairly closely 40% of the text. Therefore, in the case of the monoliteral frequency distribution of a transposition cipher, *the vowels should closely approximate 40% of the text.* For example, let us compare the percentage of vowels in the previous two cryptograms with the expected percentage of vowels in the norm:

Norm		*First Cryptogram*		*Second Cryptogram*	
Letter	*Frequency*	*Letter*	*Frequency*	*Letter*	*Frequency*
A	8	A	7	A	2
E	13	E	11	E	2
I	7	I	8	I	2
O	8	O	6	O	6
U	3	U	2	U	0
Y	1	Y	2	Y	6
	40(%)		36(%)		18(%)

It can be seen that in the first cryptogram, which has slightly less than 100 letters, the vowels constitute approximately 36% of the text. From a "quantity of vowels" viewpoint, the first cryptogram can easily be of the transposition type. However, turning to the second cryptogram, which we know *not* to be of the transposition type, the vowels constitute only 18% of the text. With such a small percentage of vowels the second cryptogram is certainly confirmed as being not of the transposition type.

Without actually making a frequency distribution, the experienced cryptanalyst can generally by a visual inspection alone determine whether or not a particular cipher-text message is of the transposition type. Not only will high frequency letters stand out, but there may be other subtle indications. For example, in the second cryptogram above the cryptanalyst notes that the letter Q has occurred four times. The cryptanalyst knows too that in normal English text the letter Q is almost invariably followed by the letter U. But in the second cryptogram there is not a single U! If the second cryptogram were of the transposition type, there should be at least four U's—one for each of the Q's. Hence, almost immediately the cryptanalyst would view with very strong suspicion the idea of the second cryptogram being of the transposition type.

Questions

1. Which letter in English generally occurs the most frequently?
2. A frequency distribution of individual letters is termed what?
3. Does it make any difference whether a frequency distribution is written out horizontally or vertically?
4. In analyzing a cryptogram what is one purpose that the monoliteral frequency distribution serves?
5. In 200 letters of normal English text, how many times would you expect the letter T to occur?
6. In 50 letters of English text, how many times would you expect the vowels (A, E, I, O, U, and Y) as a whole to occur?
7. Is the following cipher-text message of the transposition type?

```
LRYCS TDIUI SFECI TYEAT NTOIE
SENOE EIOOT IASSG AEFNR ANCDH
ESSNN NHAYV DODNG AREUP BREGO
NMOMS IIREO TLAAE HPEKI OLTH
```

8. Is the following cryptogram of the transposition type?

```
KTRSR NONCN RTKTC NRSRN RORSK
OKNKO STONC SCSRO CNCTC TRECO
ROREK OKECO RNRSS NRESS RECOO
NCOOT
```

9. The following cryptogram is believed to be of the transposition type. Is it?

```
ESARN TEAMU TYOMT EEERN DQYUO
EELQS WYETB UEOUN DTAIR RENQA
SXTSB UIOOT TPE
```

10. The cryptanalyst in solving a transposition type cipher likes to find the letter Q in the text. Why?

Chapter VI

The Biliteral Frequency Distribution

We have seen in Chapter V how the monoliteral frequency distribution is made. We have also learned how the monoliteral frequency distribution assists in the identification of a transposition type cipher system. We come now to another type frequency distribution, the *biliteral frequency distribution.*

The biliteral frequency distribution is a frequency distribution in a message of all adjacent pairs of letters, called *bigraphs.* Thus, a monoliteral frequency distribution is a count of single letters and a biliteral frequency distribution is a count of double letters or pairs of letters.

Just as we did in the case of the monoliteral frequency distribution, let us go through the steps in the construction of the biliteral frequency distribution. We are given the following cipher-text message:

```
TLOTE  IEANT  ETHAE  HFOTS  IEFBH
TRBTO  CAMRW  CAEMS  OEECH  DIEDN
TELNH  RMLIW  MLMTO
```

As in the case of making a monoliteral frequency distribution, we begin by writing out the normal alphabet. It doesn't make a great deal of difference whether the alphabet is written horizontally or vertically. However, it might be easier to visualize what we are doing, if we write the alphabet vertically as follows:

A –
B –
C –
D –
E –
F –
G –
H –
I –

J –
K –
L –
M –
N –
O –
P –
Q –
R –
S –
T –
U –
V –
W –
X –
Y –
Z –

We now start making the distribution or tabulation. The first two letters of the message are the bigraph T L. Therefore, as our first tabulation, the letter L is written to the right of the letter T in the vertical alphabet. We thus have:

A –
B –
C –
D –
E –
F –
G –
H –
I –
J –
K –
L –
M –
N –
O –
P –
Q –
R –
S –
T – L
U –
V –
W –
X –
Y –
Z –

Following the bigraph T L is the bigraph L O. Note that the letter L is the last letter of the bigraph T L as well as the first letter of the bigraph L O. Thus, continuing our tabulation, in the vertical alphabet the letter O is written to the right of the letter L. The next bigraph is O T. Hence, opposite the letter O is written the letter T. In a similar manner, letter by letter, each bigraph in the message is tabulated. With the last bigraph of the message, T O, tabulated, the completed biliteral frequency distribution looks as follows:

A – N E M E
B – H T
C – A A H
D – I N
E – I A T H F M E C D L
F – O B
G –
H – A F T D R
I – E E E W
J –
K –
L – O N I M
M – R S L L T
N – T T H
O – T T C E
P –
Q –
R – B W M
S – I O
T – L E E H S R O E O
U –
V –
W – C M
X –
Y –
Z –

It should be noted that the biliteral frequency distribution also may serve as a monoliteral frequency distribution. That is, by counting the number of letters to the right of any particular letter, you will know the number of times that that particular letter occurred in the message. For example, to the right of the letter A in the biliteral frequency distribution above are the letters N E M E. This means that the letter A occurred in the message four times. It might be noted, however, that the number of bigraphs actually tabulated is one less than the total number of letters in the message text. The reason for this of course is that the last letter of the message does not begin a bigraph and therefore no bigraph is tabulated for the last letter of the message.

How the biliteral frequency distribution is used by the cryptanalyst will be shown in the next chapter.

Questions

1. The biliteral frequency distribution also may serve as a monoliteral frequency distribution. However, one letter will appear in the monoliteral frequency distribution which does not appear in the biliteral frequency distribution. Thus, in effect the biliteral frequency distribution will have an "error" of one letter when used as a monoliteral frequency distribution. Which letter of the message does not appear in the biliteral frequency distribution?

2. Using the formula:

$$\frac{\text{Number of vowels in message}}{\text{Number of letters in message}} \times 100 = \begin{array}{c}\text{Percentage of}\\ \text{vowels in message}\end{array}$$

Compute the percentage of vowels in the following cipher-text message:

IAIOL CIOPE ATTAT EUBEA UNPRZ
SLYAP IASRO VTSIT AZOET NSLEX
HEMGR WLOET ECYIK ZRRNK OOEEO
S

3. Is the percentage of vowels in the message of Question 2 that which you would expect in a transposition type cipher?

4. Construct the biliteral frequency distribution of the following message:

PAABI CEIEH BTTLR CCNOI HOTLA
EDYTN FPETN NSWEA RSEFA GTTUU
EPDED LTNOF KASXO LHOEB E

5. What is the percentage of vowels in the message of Question 4?

6. Do you believe the message of Question 4 to be a transposition type cipher?

7. A cipher-text message contains *n* letters. How many bigraphs does the message contain?

Chapter VII

Introduction to Cryptanalysis

Given: The Plain-text Beginning of a Message Longer than the Key-length.

As an introduction to the problem of the cryptanalysis of the single columnar transposition cipher let us consider the following cipher-text message which has resulted from a single columnar transposition. The numerical key is unknown.

TTDTI TIIIH NNOBT ERNOO IGSRY
SVIAA XNAFN ASMMR IE

However, we are given the plain-text beginning of the message, the words TRANSMIT INFORMATION. The manner in which we have gained these first two words is not particularly important at this time. Perhaps this message beginning is a *stereotype* used time and again by correspondents. For that matter we might simply say that we have "guessed" this particular message beginning. In any case, if this presumed plain-text beginning does not solve the entire message, then by "trial and error" we might try another beginning until the message is finally solved. The purpose then of this chapter is merely to show how a message may be read, given the "longer than the key-length" plain-text beginning of the message.

We begin our solution by writing the cipher-text message without dividing the message into five letter groups:

T T D T I T I I I H N N O B T E R N O O I G S R Y
S V I A A X N A F N A S M M R I E

We next make a biliteral frequency distribution of the message in the manner described in Chapter VI. The distribution when made looks as follows:

A – A X F S
B – T
C –
D – T
E – R
F – N
G – S
H – N
I – T I I H G A E
J –
K –
L –
M – M R
N – N O O A A
O – B O I
P –
Q –
R – N Y I
S – R V M
T – T D I I E
U –
V – I
W –
X – N
Y – S
Z –

Let's see now how we use this biliteral frequency distribution.

Since we are given the plain-text beginning of the message, we may easily write the first few letters of the known plain-text beginning horizontally as follows:

TRANSM

Below these horizontally written letters are written the succeeding letters of the given plain-text:

T	R	A	N	S	M
R	A	N	S	M	I
A	N	S	M	I	T
N	S	M	I	T	I
S	M	I	T	I	N
M	I	T	I	N	F
I	T	I	N	F	O
T	I	N	F	O	R
I	N	F	O	R	M
N	F	O	R	M	A
F	O	R	M	A	T
O	R	M	A	T	I
R	M	A	T	I	O
M	A	T	I	O	N

In the columns which we have just made we now circle certain letters. In the first column, beneath the letter T, we circle those letters which follow T in the cipher-text message. Thus, from the biliteral frequency distribution which we have just made we see that the letter T has occurred five times; and in these five occurrences, four different letters (T, D, I, and E) have followed the letter T. Therefore, in the first column beneath the letter T we circle the letters T, D, I, and E, if they occur. We thus have the following:

T	R	A	N	S	M
R	A	N	S	M	I
A	N	S	M	I	T
N	S	M	I	T	I
S	M	I	T	I	N
M	I	T	I	N	F
Ⓘ	T	I	N	F	O
Ⓣ	I	N	F	O	R
Ⓘ	N	F	O	R	M
N	F	O	R	M	A
F	O	R	M	A	T
O	R	M	A	T	I
R	M	A	T	I	O
M	A	T	I	O	N

In a similar manner, in column two we circle the three letters N, Y, and I, since the biliteral frequency distribution shows that the letter R is followed in the cipher-text message by the three different letters: N, Y, and I. Similarly, the appropriate letters in the remaining columns are circled and the final result is the following:

T	R	A	N	S	M
R	A	N	S	Ⓜ	I
A	Ⓝ	Ⓢ	M	I	T
N	S	M	I	T	I
S	M	I	T	I	N
M	Ⓘ	T	I	N	F
Ⓘ	T	I	Ⓝ	F	O
Ⓣ	Ⓘ	N	F	O	Ⓡ
Ⓘ	Ⓝ	Ⓕ	Ⓞ	Ⓡ	Ⓜ
N	F	O	R	Ⓜ	A
F	O	R	M	A	T
O	R	M	Ⓐ	T	I
R	M	Ⓐ	T	I	O
M	A	T	I	O	N

Examining the circled letters, it is immediately noted that there is but one horizontal row in which all the letters have been circled! This is the row INFORM. Of what significance is this? It simply means that in the enciphering matrix the letters INFORM have fallen or have occurred immediately beneath the letters TRANSM. For this to have happened the key-length must be eight and the given plain-text message beginning within the matrix will look as follows:

TRANSMIT
INFORMAT
ION

Note that the letters INFORM have fallen beneath the letters TRANSM.

We can now see why in the cipher-text message the letter T is followed by the letter I. They are both from the first column to the left in the matrix. In fact, since the letters ION fall in the third horizontal row of the matrix, the first column to the left in the matrix actually begins T I I; and sure enough, looking in the cipher-text message the letters T I I are found.

Since we have found that the key-length to be 8 and we know that the number of letters in the message is 42, we can easily determine the size of the matrix used in encipherment.[1] The matrix then with its known plain-text beginning is as follows:

T	R	A	N	S	M	I	T
I	N	F	O	R	M	A	T
I	O	N					

The problem now is to identify the above eight columns in the cipher-text message. We have already mentioned finding the three letters T I I (from the first column to the left in the matrix) in the message. These three letters are known to head a column of six letters, as can be seen by looking at the matrix. Therefore, the entire column may be identified in the message:

T T D T I T I I I H N N O B T E R N O O I G S R Y
S V I A A X N A F N A S M M R I E

From the column's position in the message it is evident that this column was the second column to be taken out of the matrix during the encipherment process. Therefore, the first column to the left in the matrix is identified as Column 2 and the entire column may be put into the matrix:

2							
T	R	A	N	S	M	I	T
I	N	F	O	R	M	A	T
I	O	N					
I							
H							
N							

---

[1] See pages 12–13.

In a similar manner the remaining seven columns are easily identified in the message, and at the same time are put vertically into the matrix. We end up then with the matrix filled; and knowledge of the order in which the columns appear in the message yields the recovery of the numerical key as follows:

2	4	7	3	5	8	6	1
T	R	A	N	S	M	I	T
I	N	F	O	R	M	A	T
I	O	N	B	Y	R	A	D
I	O	A	T	S	I	X	T
H	I	S	E	V	E	N	I
N	G						

The complete plain-text message reads:

TRANSMIT INFORMATION BY RADIO AT SIX
THIS EVENING

Note that our solution has resulted in the recovery of the numerical key, and not the literal key-word itself. The recovery of the literal key-word is not within the scope of this text, though it should be mentioned that the recovery of the literal key-word, given the numerical key, is often possible. Such recovery may or may not assist in reading messages enciphered with other keys. Where there is some connecting link between key-words this recovery of actual key-words will be course be of assistance. However, because the numerical key by itself will read all messages, collectively called *traffic,* enciphered with that key, recovery of the original key-word while perhaps often desirable is not actually considered an essential element of solution.

As a final remark concerning this rather elementary solution, you can see that for this method to be successful the given or known plain-text must be longer than the key-length. The reason for this of course is that this method of solution is based on the knowledge of vertical adjacent letters within a column which are identifiable as adjacent within the cipher-text message. In order to know these adjacent letters within a column, the known plain-text must extend beyond the length of the key.

Problems

NOTE: This is the first chapter dealing with cryptanalytic technique such that problems are appropriate instead of questions. Though questions still will be used in one or two chapters to follow, problems will predominate. The problems used will be consecutively numbered.

---

1. Chicago police find the body of a man shot to death in a vacant lot. In one of his pockets are found two messages written in some sort of "code." In addition, the police find what appears to be a message written on the back of an envelope. Can you help the police in reading the two messages in "code." These are the messages:

(1) KORKN GFACO AMDGT CEMIU IPENO
NERDQ SOERS AHNGO ICIET TI

(2) BHANP OHCLE HAKTW APWRO SLVRN
DYNEU RANIT TDSMP DTOEU URIEP
ETEEE FTAIA CVSRC SESML DUONS
NO

(3) The message found on the back of an envelope:

KEEP ME INFORMED REGARDING STOCK
QUOTATIONS IN CHICAGO

2. The following message begins with the words PROCEED TO HILL:

RHIWA EAREO CLELT EKSOR ESOCO
IAVEP OFXTH TEZHE LFLYW SEZSO
IVICR NORUD IUOUT TERTX RNTHZ
NO

3. Message begins STORAGE SPACE:

TCLRB LTESG ASESE IURAH QMDPY
DSLET EALDE IBSTM LASAB NDSSE
IOEEE YEOPE PAEER NKVAV AUIGW
O

4. Message begins LATEST INFORMATION:

FAIRR OUTNI TRVSH SNEAR INTRA
ARIRD TIBTC RTEAT ASTAR TIONA
IEAMI TALPA EOLHA RONNW DIEYT
OVCCW URLAL EFLOY

5. Message begins with the word CELEBRATIONS:

ESISE FOAYH LRODC NWAHO CBIBU
UEOIA LNOEO RDTML RSEAE HRLTL
UBTNE HLSLH CTEEI OT

6. Message begins with the word ACKNOWLEDGEMENT:

KNETE EESSE EDLHE PNTSB DCGAA
CLAMT NIAEY ERPKW FAETE LMGNO
CCEMO VSOOS ESH

7. Message begins REPORT THAT:

PTCSI RELUT WEAAI EPLLO LOTSD
FHSET NORAE FTSSO UMTRT IARWB
TROHH OSEAN TORHE HCTEI EIR

8. Message begins with the word AUTOMOBILE:

MIIST SXJSD DULEG HPTOF GXOLT
OEOOU TAEAI BNTFA LYIEO WAYAI
IKREN BLIUO NCLSL RTEWB GRSCI
NA

9. Message begins with the word ADVERTISING:

VGWNT OBRAR RLNES RPSTO LTRES
AEPII TFEEN DNMIA TMPLS REEAT
OEAIA GLREP PIGBH PPTR

10. Message begins with the word TRANSPORTATION:

RNGII OBRUD ARTRH NIDEN PLOOW
TRHII REBAE AWEMN SLFYE TAYRL
IAEVT ONTE

Chapter VIII

The Analytic Matrix

In the last chapter we learned how to solve a single columnar transposition cipher given an amount of beginning plain-text greater than the length of the key. The method of solution presented was rather simple and in fact was almost mechanical. Unfortunately, however, in solving a cipher-text message, it is generally the exception rather than the rule that you will know the beginning plain-text. Therefore, other cryptanalytic means must be employed in order to read messages. So it is that our methodology brings us to more complicated aspects in the solution of the single columnar transposition cipher.

If you remember before the method of solution was presented in the last chapter, several tools of the cryptanalyst were presented in earlier chapters.[1] Similarly, in this chapter we are going to present "before going into deeper waters" another tool of the cryptanalyst. This tool, an important one, is termed the *analytic matrix*.

The analytic matrix in certain respects may be said to form the foundation for the cryptanalytic solution of all columnar transposition cipher systems. In order to construct the analytic matrix for a particular cipher-text message you need but one thing besides the cipher-text itself—the key-length. Therefore, given a cipher-text message and the key-length let us follow the steps in the construction of the analytic matrix.

The message:

```
EIPEI  EUFSS  ETODE  ERTJR  OOSCL
NTPLH  EDGRF  TEEEE  SAOIT  SNULP
VONPT  ADAEL  YVLT
```

The key-length: 10

---

[1] The monoliteral and biliteral frequency distributions.

The *first step* in the construction of the analytic matrix is to determine the size of the enciphering matrix, and more particularly to determine the *number of long columns* and the *number of short columns* as well as the *length of a long column* and the *length of a short column.* We are given the key-length, in this case 10; and by merely counting the number of letters in the cipher-text message, we can determine the message length, in this case 64. With the key-length and the message length we can easily compute the size of the enciphering matrix.[1] Thus we know that the message above is divided into four long columns of length 7 and six short columns of length 6. We usually express this in short form as follows:

$$64 = \frac{4-7'\text{s}}{6-6'\text{s}}$$

The short form is verified at a glance, since 4×7=28 plus 6×6=36 equals the length of the message 64.

After determining the size of the enciphering matrix our *second step* is to divide the cipher-text message into long and short columns with the long columns going at the head of the message and the short columns at the tail of the message:

EIPEI EU/FSS ETOD/E ERTJR O/OSCL
NTP/LH EDGR/F TEEEE/SAOIT S/NULP
VO/NPT ADA/EL YVLT

Thus the first 28 letters of cipher-text are divided into four long columns and the last 36 letters of cipher-text are divided into six short columns.

The *third step* of our analytic matrix construction is to write down vertically from left to right these divided columns, *keeping the bottoms of the columns on the same line.* Thus:

---

[1] See pages 12-13.

$$\begin{array}{cccccccccc}
E & F & E & O & & & & & & \\
I & S & E & S & L & F & S & N & N & E \\
P & S & R & C & H & T & A & U & P & L \\
E & E & T & L & E & E & O & L & T & Y \\
I & T & J & N & D & E & I & P & A & V \\
E & O & R & T & G & E & T & V & D & L \\
U & D & O & P & R & E & S & O & A & T
\end{array}$$

These letters are the foundation of the analytic matrix. The *fourth and last step* is to extend the tops of the columns from right to left such that the long columns come at the tail of the message and the short columns at the head of the message. We begin by drawing a line across the top of the present columns:

$$\begin{array}{cccc|cccccc}
\overline{E} & \overline{F} & \overline{E} & \overline{O} & & & & & & \\
I & S & E & S & \overline{L} & \overline{F} & \overline{S} & \overline{N} & \overline{N} & \overline{E} \\
P & S & R & C & H & T & A & U & P & L \\
E & E & T & L & E & E & O & L & T & Y \\
I & T & J & N & D & E & I & P & A & V \\
E & O & R & T & G & E & T & V & D & L \\
U & D & O & P & R & E & S & O & A & T
\end{array}$$

Starting with the short columns on the right we now make the columns long. Thus, the first short column on the right is made long by adding one additional letter which comes from the bottom of the adjacent column to the left. Above the letter in the adjacent column is drawn a line. We thus have:

$$\begin{array}{cccc|cccccc}
\overline{E} & \overline{F} & \overline{E} & \overline{O} & & & & & & A \\
I & S & E & S & \overline{L} & \overline{F} & \overline{S} & \overline{N} & \overline{N} & \overline{E} \\
P & S & R & C & H & T & A & U & P & L \\
E & E & T & L & E & E & O & L & T & Y \\
I & T & J & N & D & E & I & P & A & V \\
E & O & R & T & G & E & T & V & D & L \\
U & D & O & P & R & E & S & O & \overline{A} & T
\end{array}$$

The next column, still going from right to left, is made long by adding two letters at the top which, as in the case of the first column, come from the bottom of the adjacent column to the left. Again, above these two letters in the adjacent column is drawn a line. Thus:

```
                  V
E F E O|          O A
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P A V
E O R T G E T V D L
U D O P R E S O A T
```

Note that the lines being drawn above the letters on the bottoms of the columns are an aid to extending the columns above, *since above the drawn line will be a column length.* So far we have made two short columns into long columns. We extend two more short columns making a total of four extended long columns:

```
            E
            E I
            E T V
E F E O|    E S O A
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P A V
E O R T G E T V D L
U D O P R E S O A T
```

At this point, still going from right to left, we extend the remaining columns, not however into long columns, but into the remaining six short columns. Thus, in the next column to the left only four letters are added to the top of the column. This extends the column *above the drawn line* the length of only a short column. As was the case with the other columns, a line is drawn above the four letters in the adjacent column to the left. We have then:

```
          E E
          D E I
          G E T V
E F E O|  R E S O A
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P A V
E O R T G E T V D L
U D O P R E S O A T
```

In a similar manner the remaining columns are extended the length of a short column *above the drawn line,* and the final completed analytic matrix looks as follows:

```
      J L E E
    O R N D E I
  U D O T G E T V
E F E O|P R E S O A
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P A V
E O R T G E T V D L
U D O P R E S O A T
```

Note that the lengths of the columns—above the drawn lines at the bottoms of the columns—are from right to left the four long columns and then the six short columns.

Just what does this *analytic matrix* represent?

The analytic matrix represents the columns of the enciphering matrix in numerical order from left to right, thus:

```
   Numerical Key
1 2 3 4 5 6 7 8 9 10
--------------------
      J L E E
    O R N D E I
  U D O T G E T V
E F E O|P R E S O A
I S E S L F S N N E
P S R C H T A U P L
E E T L E E O L T Y
I T J N D E I P A V
E O R T G E T V D L
U D O P R E S O A T
```

Because we do not know which columns are actually long columns and which are actually short columns, the columns of the analytic matrix will contain superfluous letters which belong in an adjacent column. However, regardless of how the long and short columns are arranged in the actual enciphering matrix, *the columns of the analytic* *matrix will contain all the letters of the columns as found in the actual enciphering matrix.*

The analytic matrix will be used frequently in chapters to come; and the student should be able to quickly construct the analytic matrix, given only a message and key-length.

Questions

1. In order to construct an analytic matrix you need but one thing beside the message itself. What is it?

2. What is the *first step* in the construction of the analytic matrix?

3. What is the *second step*?

4. What is the *third step*?

5. What is the *fourth step*?

6. Construct the analytic matrix of the following message, given the key-length 9:

   IHAST TMXML SHDLY GITEU DAARI
   DELUI ASOEV GLOTO ESEEB SRYTU
   SEWDN UTRSC NELAH LERIA TREXA
   E

7. Construct the analytic matrix of the following message, given the key-length 6:

   EAASP LIIEN SQSNO OERET SSBUS
   COSRS AAI

8. Construct the analytic matrix of the following message, given the key-length 8:

   UQEGO DTNAO EUVHS OEIEY QSRUT
   TR

Chapter IX

Cryptanalytic Solution

Given : Plain-text Longer than the Key-length Anywhere in the Message.

We have already considered in Chapter VII the problem of cryptanalytic solution, given the "longer than key-length" plain-text beginning of a message. In this chapter we are going to take up the same problem with one exception—the known plain-text does not specifically have to be at the beginning of the message. Instead, the known plain-text may be anywhere in the message. Note, however, that the condition that the plain-text must be longer than the key-length still exists.

Let us go through the solution of a typical problem. We are given a cryptogram with the name of the ship QUEEN ELIZABETH suspected to be therein:

```
BIEEH  VHBSR  UAHEE  OREBE  ECOWV
NTETM  TAQZT  TDRNI  EESNE  ELOLO
EOERL  NINNF  R
```

Our first step is to find the key-length of the enciphering matrix. To do this we follow the same procedure as in the case of the problem in Chapter VII. Thus we begin by making a biliteral frequency distribution of the message:

```
A – H Q
B – I S E
C – O
D – R
E – E H E O B E C T E S E L O R
F – R
G –
H – V B E
I – E E N
J –
```

K–
L–OON
M–T
N–TIEINF
O–RWLEE
P–
Q–Z
R–UENL
S–RN
T–EMATD
U–A
V–HN
W–V
X–
Y–
Z–T

With the biliteral frequency distribution constructed, just as we did in Chapter VII, we write horizontally the first few letters of our given or known plain-text:

QUEEN

Beneath these letters succeeding letters of plain-text are written:

Q	U	E	E	N
U	E	E	N	E
E	E	N	E	L
E	N	E	L	I
N	E	L	I	Z
E	L	I	Z	A
L	I	Z	A	B
I	Z	A	B	E
Z	A	B	E	T
A	B	E	T	H

In the columns thus extended those letters are circled which follow the top column letter in the biliteral frequency distribution. The result is the following:

Q U E E N

U E Ⓔ N Ⓔ
E E N Ⓔ L
E N Ⓔ Ⓛ Ⓘ
N E Ⓛ I Z
E L I Z A
L I Z A B
I Z A Ⓑ Ⓔ
Ⓩ Ⓐ Ⓑ Ⓔ Ⓣ
A B Ⓔ Ⓣ H

Examining the circled letters it is immediately seen that the row **Z A B E T** is the only one in which all the letters have been circled. This indicates that in the enciphering matrix the letters **Z A B E T** have fallen directly under the letters QUEEN; and for this to have happened the key-length must be eight, i.e.,

$$\begin{array}{l} \underline{\text{QUEEN}}\text{ELI} \\ \underline{\text{ZABET}}\text{H} \end{array}$$

Note that up to this point our cryptanalytic procedure has been exactly as that in Chapter VII. However, our technique now changes.

Knowing the key-length to be eight we are now able to construct the *analytic matrix* of the message:

$$\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\
 & & & C & M & & & \\
 & & E & O & T & R & & \\
 & B & O & W & A & N & E & \\
B & S & R & V & Q| & I & L & R \\
I & R & E & N & Z & E & O & L \\
E & U & B & T & T & E & L & N \\
E & A & E & E & T & S & O & I \\
H & H & \underline{E} & \underline{T} & \underline{D} & N & E & N \\
V & \underline{E} & C & M & R & \underline{E} & O & N \\
\underline{H} & E & O & T & N & E & \underline{E} & F \\
B & O & W & A & I & L & R & R
\end{array}$$

Our next step is to *juxtapose* or to rearrange the columns of the analytic matrix to agree with the already known portion of the enciphering matrix:

Q U E E N E L I
Z A B E T H

This is not a difficult task. For example, the vertical letters $\begin{smallmatrix}Q\\Z\end{smallmatrix}$ are easily identified as being in Column 5 of the analytic matrix and the vertical letters $\begin{smallmatrix}U\\A\end{smallmatrix}$ as being in column 2. Therefore, these two particular columns may be juxtaposed as follows:

5	2						
M	B						
T	S						
A	R						
Q	U	E	E	N	E	L	I
Z	A	B	E	T	H		
T	H						
T	E						
D	E						
R	O						
N							
I							

In a similar manner the remaining columns are easily identified and added to the juxtaposition:

5	2	3	6	4	1	7	8
				C			
M	B	E	R	O	B	E	R
T	S	O	N	W	I	L	L
A	R	R	I	V	E	O	N
Q	U	E	E	N	E	L	I
Z	A	B	E	T	H	O	N
T	H	E	S	E	V	E	N
T	E	E	N	T	H	O	F
D	E	C	E	M	B	E	R
R	O	O	E	T		R	
N		W	L	A			
I							

By inspection of the resulting juxtaposition it is evident that the plain-text message of 61 letters lies within the juxtaposition as follows:

5	2	3	6	4	1	7	8
				C			
M	B	E	R	O	B	E	R
T	S	O	N	W	I	L	L
A	R	R	I	V	E	O	N
Q	U	E	E	N	E	L	I
Z	A	B	E	T	H	O	N
T	H	E	S	E	V	E	N
T	E	E	N	T	H	O	F
D	E	C	E	M	B	E	R
R	O	O	E	T		R	
N		W	L	A			
I							

The superfluous letters are eliminated; and keeping the order of the columns the same, Column 6—containing the first letter of the plain-text message—is put on the left. The result is the original enciphering matrix and numerical key.

6	4	1	7	8	5	2	3
R	O	B	E	R	T	S	O
N	W	I	L	L	A	R	R
I	V	E	O	N	Q	U	E
E	N	E	L	I	Z	A	B
E	T	H	O	N	T	H	E
S	E	V	E	N	T	E	E
N	T	H	O	F	D	E	C
E	M	B	E	R			

And the plain-text message is:

> ROBERTSON WILL ARRIVE ON QUEEN ELIZABETH ON THE SEVENTEENTH OF DECEMBER

Several remarks may be made regarding this cryptanalytic solution. The student should note that in the process of juxtaposing the columns of the analytic matrix, in addition to merely identifying columns by the known plain-text portion of the enciphering matrix, use can and should be made of combinations of plain-text letters that appear on other rows of the analytic matrix. In other words, proper juxtaposition of columns of the analytic matrix depends not only upon the known plain-text portion of the enciphering matrix, but also upon plain-text appearing on other horizontal rows.

It should also be noted that this method of cryptanalytic solution does not depend upon the known plain-text being located at any particular point within the message. Thus, this method may be used with success even though, for example, the known plain-text may turn out to be at the beginning of the message. In other words, this is a more general solution than that of Chapter VII.

Problems

11. The following message contains the words PRESIDENT JACKSON:

AANXO RAHOE AERYD SKCDC SIECP
JTOST LCTRE CEREL NCOTF GUGIS
RGENC HLSEE IISHE OWAAN DOIRU
LEATN OAO

12. The following message contains the words LOS ANGELES CALIFORNIA:

CLNNE PEDFH LOYPI ORLSA EYGNI
AGOFO ISOTT AEELI SDOTC NLUNY
ANEEA TEOTO BGINR GSEEE NSLNP
LARWO RNEDC UCITW OFTSU T

13. The following message contains the word CONDITION:

WEETC TIDSE PRERI SDASR UOOIN
LTPSP VNOME NAASE DNIE

14. The following message contains the words PLEASE ADVISE:

VEFAC BLICN ARPTE EELST OAEDR
NEEES RNODS RAEEO MEESS HIWEI
EPDAV SXNMP V

15. The following message contains the word ACKNOWLEDGE:

EOGDT WENNP FOLAT NOHKE DCRLP
ESDEO IADES CNESO LARPG CGAIS
TNP

16. The following message contains the words RECEIVE INSTRUCTIONS:

CWISE OPTPR RRLTT HHTNA ANIEU
EFION SELRE NEMSB AOIAE TIHHH
OOIDR RHOWT ILTAO VOTSE OCMPT
IIFIR EFPOI NONNE AIECN CCFTT
TGTRP OLSNT TCITL

17. The following message contains the words SAN FRANCISCO:

RRTRP ETHSV CGOIU ABRAE TEERI
ISSTL DPYAF AIKVN SLACT OHMTU
INIYR QEPLN OHCAE OWEIH COID

18. The following message contains the words TWO THOUSAND:

TLLUL ESLNO EMTUS AVILS TTDRT
EEOOR DLBHJ WAEEA EISNE ARWBT
EIYAQ ESIDT IUHDM

19. The following message contains the words TELEPHONE CALL:

TLECT NNOIA COOCD HEIEN VYABT
EEWTR BPCRD MLNEE ENTLA HEDIR
NEAYI SEOLR TIAIL ELSHH WP

20. The following message contains the words CALIFORNIA ORANGES:

AGHEE TSISE TURRO NEOEO NNRET
HTECN TNBRN EFOLM RCAIR UOOHS
ULEEX SEUIA NHAAC HOOHT CNAPA
TFPAI SROVN TNCSA BTSTI L

Chapter X

Cryptanalytic Solution

Given: The Key-length and a Completely Filled Matrix.

In Chapter III it was stated during discussion of the "encipherment" of the single columnar transposition cipher that matrices were divided into two types:

(1) The in-completely filled matrix.
(2) The completely filled matrix.

Up to this point we have not seriously considered the possibility of correspondents employing the columnar transposition cipher using a completely filled matrix. In fact, almost all examples and problems up to this chapter have been of the in-completely filled matrix type.

To the cryptanalyst the completely filled matrix type columnar transposition cipher is by far much simpler of solution than the in-completely filled matrix type. The reason for this briefly is that the completely filled matrix type columnar transposition cipher has but one column length. Thus, there is no problem of long columns and short columns to contend with. Exactly why but one column length helps the cryptanalyst will be brought out in this chapter.

The reason that the completely filled matrix type problem is taken up for the first time now is that this chapter introduces the student to the cryptanalytic technique termed *column matching*. Because column matching is greatly facilitated when column lengths are known, the completely filled matrix type problem is ideal to use when introducing this technique.

Therefore, let use solve the following cryptogram, given the key-length of six:

GLLEF PLUOT HERPI RDEBC NLGEE
NNBAR SETHO TEYWP EHIAO LIRMC
SERTS VIIEH EALPO OEAFW TX

The message length is 72 letters. Since the given key-length of six goes into the message length evenly (12 times), the enciphering matrix is a completely filled matrix with a column length of 12. Thus, the analytic matrix for the message is as follows:

1	2	3	4	5	6
G	R	E	E	M	E
L	P	N	Y	C	A
L	I	N	W	S	L
E	R	B	P	E	P
F	D	A	E	R	O
P	E	R	H	T	O
L	B	S	I	S	E
U	C	E	A	V	A
O	N	T	O	I	F
T	L	H	L	I	W
H	G	O	I	E	T
E	E	T	R	H	X

Compare this analytic matrix (with but one column length) with the analytic matrix constructed for a message enciphered with an in-completely filled enciphering matrix.[1]

Solution depends now merely upon re-arranging these six columns into *numerical key* order!

The cryptanalyst has in general two lines of attack in the re-arrangement of these columns. He may use the technique of *anagramming* expected combinations of letters. Thus, for example, he may find the letter Q on a row. Since the letter Q is almost invariably followed by the letter U, there should be a letter U on the same row—unless by chance the column with the letter Q is the right hand column, in which case the column with the letter U will be the left hand column and the letter U therefore will be on the row beneath the row containing the letter Q. Thus, the column containing the letter Q may be placed in front of the column containing the letter U. This placing of one column next to another column is termed *column matching* or *column juxtaposing*. In addition to the bigraph QU, the cryptanalyst might also use other "good" combinations of letters, such as CK, TH, etc. Also the cryptanalyst might attempt to anagram common or expected words or portions of words using letters from one row. The cryptanalyst's second line of attack is more general and does not by itself depend upon anagramming or the guessing of letter combinations. This second line of attack is particularly important and will be presented in some detail.

---

[1] See Chapter VIII.

One column is selected, say for example, Column 1 from the analytic matrix above:

1
G
L
L
E
F
P
L
U
O
T
H
E

Unless by chance this Column 1 is the right hand column of the enciphering matrix, to the right of Column 1 will stand one of the remaining five columns. Thus, there are five possible juxtapositions:

1 2	1 3	1 4	1 5	1 6
G R	G E	G E	G M	G E
L P	L N	L Y	L C	L A
L I	L N	L W	L S	L L
E R	E B	E P	E E	E P
F D	F A	F E	F R	F O
P E	P R	P H	P T	P O
L B	L S	L I	L S	L E
U C	U E	U A	U V	U A
O N	O T	O O	O I	O F
T L	T H	T L	T I	T W
H G	H O	H I	H E	H T
E E	E T	E R	E H	E X

Letter Contact Weight Chart

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A		2	2	1		1	1		1	1	1	2	1	3		2		2	2	2		2	1	1	1	
B	1	1			4				1			2			1			1			2				1	
C	2				2			2	1		2	1			2			1		1	1					
D	2			1	2	1			2	1					1			1			1	1			1	
E	2		1	2		1	1					1	1	2		1	2	2	2			1	1	3		
F	1				1	1			1			1			2			1		1	1					
G	1				2			2	1			1			2			2			1					
H	3				4				2						2					1						
I	1	1	2	1	1	2	1				2	2	1	3	2			1	2	2		2		2		
J	1				1										2						1					
K	1				3				2					1	1				1						1	
L	2			2	3				2		1	2			2				1	1	1				3	
M	3	1			3				2				1		2	1					1					
N	1		1	2	1		2		1	1	1			1	1				1	2	1	1		1	1	
O	1	1	1	1		3	1		1		2	1	2	3	1	2		2	1	2	3	2	2	1		
P	2				2			1	1			2			2			2		1	1					
Q																					5					
R	1			1	2		1		1		1	1	1		1					1	1	1				
S	2				2			2	2		1	1	1	1	2	2	1		1	3	2		1			
T	2				2			4	3						3			1	1	2	2		1			
U	1	1	1	1	1		1					1	1	2		1		2	2	2						
V	2				4				2						2											
W	2				2			3	2						1											
X	1		1		1				1						1	1				1						
Y	1				1										2											
Z					3										2											

To find the weight of a given bigraph, the first letter of the bigraph is found in the vertical column of letters on the left side of the chart and the second letter of the bigraph is found in the horizontal row of letters at the top of the chart. At the intersection of these letters will be found the weight of the bigraph. Thus, the bigraph QU has a weight of 5, WH has a weight of 3, etc.

FIGURE 3.

The question now is which of these five possibilities is more likely to be the correct matching of columns? To answer this question we employ a "letter contact weight chart." This "letter contact weight chart" is shown as Figure 3 on the reverse page. The weights given in this chart are somewhat general in nature and the particular weights given are roughly dependent upon the expected frequency of occurrence of the bigraphs plus the concept of "good" bigraphs such as QU, LY, CK, TH, etc. The manner in which this "letter contact weight chart" is used is as follows.

Each of the five possible juxtapositions consists of a column of 12 bigraphs. These bigraphs have certain "weights" as determined by the "letter contact weight chart."[1] These various weights are then tabulated and a total weight, termed the *validity* weight, is obtained for each possibility. This tabulation is as follows:

1 2		1 3		1 4		1 5		1 6	
GR	2	GE	2	GE	2	GM	0	GE	2
LP	0	LN	0	LY	3	LC	0	LA	2
LI	2	LN	0	LW	0	LS	1	LL	2
ER	2	EB	0	EP	1	EE	0	EP	1
FD	0	FA	1	FE	1	FR	1	FO	2
PE	2	PR	2	PH	1	PT	1	PO	2
LB	0	LS	1	LI	2	LS	1	LE	3
UC	1	UE	1	UA	1	UV	0	UA	1
ON	3	OT	2	OO	1	OI	1	OF	3
TL	0	TH	4	TL	0	TI	3	TW	1
HG	0	HO	2	HI	2	HE	4	HT	1
EE	0	ET	0	ER	2	EH	0	EX	3
	12		15		16		12		23

Examining the validity weights of each of these possible matched columns we find that the most favorable possibility is that of Column 6 being to the right of Column 1. That is, the 12 bigraphs formed by the juxtaposition of Column 6 to the right of Column 1 are "as a whole" bigraphs with higher weights than bigraphs in the other possible matched columns. In fact, the experienced cryptanalyst can almost *visually* look at matched columns and with a high degree of accuracy determine their validity. However, the "letter contact weight chart" is often of assistance even to the experienced cryptanalyst.

---

[1] How to find the weight of a specific bigraph is shown at the bottom of the "letter contact chart".

Thus far, we have determined almost "mechanically" that the most favorable possibility in the matching of these columns is that Column 6 is juxtaposed to the right of Column 1. We might continue solution by matching other columns using only validity weights. However, the cryptanalyst normally uses simultaneously both his lines of attack[1] in re-arranging the columns of the analytic matrix. Thus, for example, it is noted in the two columns already matched that the bigraph LL is in the third row from the top. In English the combination of letters LL is normally preceded by a vowel. Therefore, with this in mind let us examine the analytic matrix and see which column might go in front of Column 1.

The Analytic Matrix				Columns Already Matched		
2	3	4	5	1	6	
R	E	E	M	G	E	
P	N	Y	C	L	A	
I	N	W	S	L	L	3rd row
R	B	P	E	E	P	
D	A	E	R	F	O	
E	R	H	T	P	O	
B	S	I	S	L	E	
C	E	A	V	U	A	
N	T	O	I	O	F	
L	H	L	I	T	W	
G	O	I	E	H	T	
E	T	R	H	E	X	

The only vowel available to precede the bigraph LL is the letter I in Column 2.[2] Therefore, let us place Column 2 to the left of Column 1:

---

[1] (1) *Anagramming* expected combinations of letters and (2) using the "letter contact weight chart".

[2] This is with the assumption, of course, that column 1 is *not* the left hand column of the enciphering matrix. If by chance column 1 is the left hand column, the vowel necessary to precede the letters LL would come then from the next higher row, i.e., row 2.

2	1	6
R	G	E
P	L	A
I	L	L
R	E	P
D	F	O
E	P	O
B	L	E
C	U	A
N	O	F
L	T	W
G	H	T
E	E	X

Visually the three matched columns look pretty good. Note particularly such good trigraphs as BLE, GHT, etc. We may presume therefore that the columns are correctly matched. The student himself may finish matching the remaining three columns in the same manner, using simultaneously the "letter contact weight chart" and the technique of anagramming expected combinations of letters.

The final correct juxtaposition of the columns of the analytic matrix yields the original enciphering matrix:

3	5	4	2	1	6
E	M	E	R	G	E
N	C	Y	P	L	A
N	S	W	I	L	L
B	E	P	R	E	P
A	R	E	D	F	O
R	T	H	E	P	O
S	S	I	B	L	E
E	V	A	C	U	A
T	I	O	N	O	F
H	I	L	L	T	W
O	E	I	G	H	T
T	H	R	E	E	X

And the original plain-text message is:

EMERGENCY PLANS WILL BE PREPARED FOR THE POSSIBLE EVACUATION OF HILL TWO EIGHT THREE X

A few final remarks are in order, particularly with respect to the reliability of the validity weights in column matching. As a general statement we may say that the longer the columns, the more reliable become the validity weights of the columns matched. Generally speaking, a random bigraph—from a mis-matched juxtaposition—has a weight of 1. Thus, a mis-matched pair of columns of length 10 will yield an "on-the-average" validity weight of 10. On the other hand, a valid bigraph—from a correctly matched juxtaposition—has an average weight of 1.5. Therefore, if the column length of of a pair of correctly matched columns is 10, the validity weight of the matching "on-the-average" will be 15. These values of 1 for a random bigraph and 1.5 for a valid bigraph are only approximate and a different "letter contact weight chart" will of course give rise to different on-the-average random bigraph and valid bigraph values.

Finally, it should be stated that column matching is not something which is entirely "mechanical." In fact, it is probably more of a learned "art" rather than a "science." The student must practice to become proficient and the secret of success as in may lines of endeavor may be expressed in the three words "don't give up!"

Problems

21. The following cryptogram has a key-length of 13:

CENSH OLOEI BVOGA AANER ABJER
INRTE CSOTW AATRA HESFE SNLNA
TDSPA PSLET CIEMA LTILP EAKOS
BROOR EOWRF RIOHA SRSEC OLAGF
CHSNR APLFR GSSDP FSSUI IDORI
PEEOS TDONI ADNPM ASSRM NOITR
OSNOI Y

22. The following cryptogram has a key-length of 12:

QCESO DOFDA OEAMA ETERH LFGAO
AWUHM NAOTE ESCJO EABBO SSTKO
PCGES ETEEU LUENH NSRAT HHSEA
EJUHN TTOTO TRFAH THSBT OETTR
NBHQL QRECE TLDEI ETRTS OESPT
INEMT KP

23. The following cryptogram has a key-length of 7:

TTIHR TPLNA STSRE FTNDO EEAST
PPUOT IMRMU MAEEG EFTRP EUVDS
EERHC TOOYO IUYFN OEQNH VLRNO
OU

24. The following cryptogram has a key-length of 9:

AUEWC MFIHO TOIOE HIEXE SRWLR
TTJIR NELEP CNTIT DEOTT LRETN
ACLWS EOCEE RRFIT PPNTO DDBDE
OONGW PSLHO EOSHE

25. The following cryptogram has a key-length of 8:

SRPBA RRIUF UAROU EIOPS WUARI
MLERH TOQNS HOYQP RIREN EARTO
IEDEE DEOES FDDS

26. The following cryptogram has a key-length of 9:

CIODI IPSPH IRCME IOCEH ATTVR
UDHCR ONNFN EAILA NMEBC LNLFA
DOEOH WTONG RFRRT RRXAN GAIEO
LTOOI COIEL REEKS

27. The following cryptogram has a key-length of 9:

XAUCI GTEET WATPC NEITT DIDYT
BDSST CTEND ITERL MHTEM ALIIP
TNKNH EEHOA GIA

28. The following cryptogram has a key-length of 11:

IEMWD SHRKA TETAF ETRYT RASLR
ITEEU SMREF ULPOR TDBEQ ELOHS
QAETE

29. The following cryptogram has a key-length of 11:

APXAI IKCTA ODSGS PEHLT IEAAE
EOAWA RVVNE ASSTY IIHEE SGVBN
BCAEE GELKY PRDKO RPEIM DDGDG
NY

30. The following cryptogram has a key-length of 7:

CIGDW WESRT NCTLY OTINS ANKTE
LETDF AEREC AHOTW UNEII AMTNL
IEREN S

Chapter XI

Identification of the " Completely Filled Matrix "

Chapter X covered the solution of the single columnar transposition cipher where the cryptanalyst was given the key-length plus the added condition that the enciphering matrix be a "completely filled matrix." Since solution of the single columnar transposition cipher system is relatively easy when the enciphering matrix is completely filled—as compared to the in-completely filled matrix—the cryptanalyst should not overlook the possibility that correspondents might be using completely filled matrices. The use of completely filled matrices may be intentional with every message or perhaps might simply be the result of chance. In any case, there are means for the cryptanalyst to identify cryptograms which have been enciphered with completely filled matrices. These means, however, unfortunately do not always give positive results. That is, by an examination of the cryptogram the cryptanalyst cannot always state flatly yes or no, whether or not a particular message is the result of a completely filled matrix. On the other hand, quite often the results are negative. That is, often the cryptanalyst can definitely rule out the possibility of a completely filled matrix. Finally, of course, the results may be indefinite. However, the means used by the cryptanalyst in testing for the use of a completely filled matrix are valuable, and this is the subject of this chapter.

Let us begin by taking a look at another tool of the cryptanalyst. This tool is a table titled "Table of Key-Lengths and Column-Lengths of Completely Filled Matrices—Given the Message-Length." This table is shown as Figure 4 beginning on page 70.

Using this table the cryptanalyst is able to determine whether or not a particular message *might have been* enciphered with a completely filled enciphering matrix. In other words, the table lists the sizes or dimensions of enciphering matrices given the message length plus the condition that the enciphering matrix be completely filled. It must be realized, however, that simply because the table indicates that the length of a particular message is a length which might have come from a completely filled matrix, the message does not necessarily actually have had to have resulted from a completely filled matrix.

Just where does this leave the cryptanalyst? First of all, the table indicates that certain lengths (about 30% of all lengths) cannot have resulted from completely filled matrices. Secondly, as previously stated at the beginning of this chapter, the cryptanalyst does have means to test completely filled analytic matrices for validity without actually reading the message! This testing is in fact the crux of this chapter.

Let's examine an actual example. We are given the following cipher-text message which we suspect is the result of a completely filled enciphering matrix. The key-length is unknown.

URIRT PEGRV ATEPI AFZSS ITLFU
MAHKI ECOLT CWVAW PEYLO RAESL
ERETO M

Looking up the message length (56) in the table of Figure 4 on page 71, we find that the message might indeed be the result of a completely filled enciphering matrix. Further, if the message is the result of a completely filled enciphering matrix, the key-length must be either 4, 7, 8, or 14.

Thus, the four possible completely filled analytic matrices are the following:

(7×8)

1	2	3	4	5	6	7
U	R	F	U	O	P	S
R	V	Z	M	L	E	L
I	A	S	A	T	Y	E
R	T	S	H	C	L	R
T	E	I	K	W	O	E
P	P	T	I	V	R	T
E	I	L	E	A	A	O
G	A	F	C	W	E	M

(14×4)

1	2	3	4	5	6	7	8	9	10	11	12	13	14
U	T	R	E	F	I	U	K	O	W	P	O	S	E
R	P	V	P	Z	T	M	I	L	V	E	R	L	T
I	E	A	I	S	L	A	E	T	A	Y	A	E	O
R	G	T	A	S	F	H	C	C	W	L	E	R	M

(4×14)

1	2	3	4
U	I	K	Y
R	A	I	L
I	F	E	O
R	Z	C	R
T	S	O	A
P	S	L	E
E	I	T	S
G	T	C	L
R	L	W	E
V	F	V	R
A	U	A	E
T	M	W	T
E	A	P	O
P	H	E	M

(8×7)

1	2	3	4	5	6	7	8
U	G	I	T	K	C	Y	L
R	R	A	L	I	W	L	E
I	V	F	F	E	V	O	R
R	A	Z	U	C	A	R	E
T	T	S	M	O	W	A	T
P	E	S	A	L	P	E	O
E	P	I	H	T	E	S	M

By testing each of these analytic matrices in turn *without actually reading the message* we may obtain the reliability or validity of each these particular key-lengths.

The test which we shall use is based upon the fact that in normal plain-text approximately 40% of the letters are vowels; and further, *that these vowels will be evenly distributed throughout the text!*

Let's start by testing the key-length 14. The analytic matrix is written out and the number of vowels on each row or line are counted:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	Number of Vowels
Ⓤ	T	R	Ⓔ	F	Ⓘ	Ⓤ	K	Ⓞ	W	P	Ⓞ	S	Ⓔ	7
R	P	V	P	Z	T	M	Ⓘ	L	V	Ⓔ	R	L	T	2
Ⓘ	Ⓔ	Ⓐ	Ⓘ	S	L	Ⓐ	Ⓔ	T	Ⓐ	Ⓨ	Ⓐ	Ⓔ	Ⓞ	11
R	G	T	Ⓐ	S	F	H	C	C	W	L	Ⓔ	R	M	2
														22

Note that for convenience in counting the vowels are circled.

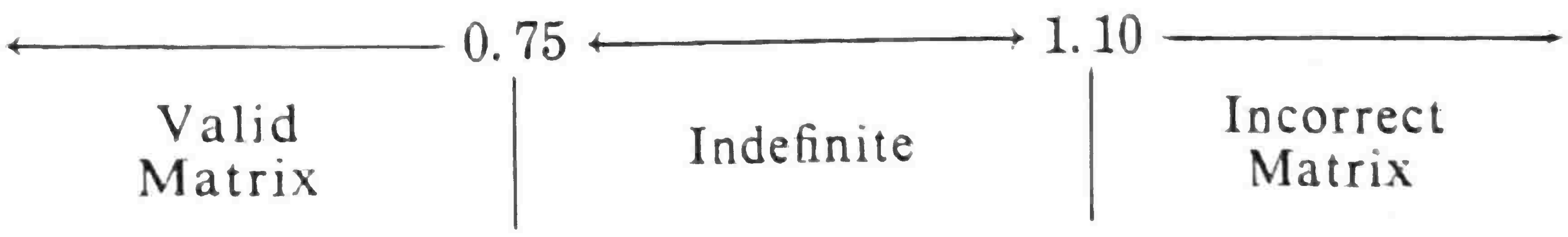
The total number of vowels in the matrix is 22. Therefore, since there are four rows, *and if this is a valid analytic matrix,* there should be 22/4 or 5.5 vowels on each row. This is with the premise, of course, that the vowels are *evenly* distributed in the plain-text. This 5.5 (number of vowels) we call the *expected mean* for each row. We now shall tabulate for each row the difference between the expected mean (in this case 5.5) and the actual number of vowels found. This difference is called the *mean difference.*[1] We also will tabulate the total of the mean differences. Thus:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	Number of Vowels	Mean Difference
Ⓤ	T	R	Ⓔ	F	Ⓘ	Ⓤ	K	Ⓞ	W	P	Ⓞ	S	Ⓔ	7	1.5
R	P	V	P	Z	T	M	Ⓘ	L	V	Ⓔ	R	L	T	2	3.5
Ⓘ	Ⓔ	Ⓐ	Ⓘ	S	L	Ⓐ	Ⓔ	T	Ⓐ	Ⓨ	Ⓐ	Ⓔ	Ⓞ	11	5.5
R	G	T	Ⓐ	S	F	H	C	C	W	L	Ⓔ	R	M	2	3.5
													total =	22	14.0

Since the total of the mean differences is proportional to the number of rows, by dividing this total by the number of rows, we will obtain an average mean difference for one row. This value is termed the *validity value of the matrix.* Thus in the present case, the total of the mean differences (14.0) divided by the number of rows (4) is equal to 3.50 which is the *validity value of the matrix.*

We know now how to obtain the validity value of the matrix, but how do we interpret the particular value which we obtain? To answer this question a considerable number of tests have been made and the results are substantially as follows:

Validity Values



In the indefinite range, from the value 0.75 to the value 1.10, the more closely that a tabulated validity value is to 0.75, the more likely it is that the matrix is valid. Conversely, the more closely that a tabulated value is to 1.10, the more likely it is that the matrix is incorrect.

---

[1] Also termed *deviation from the mean.*

In the case of the analytic matrix which we have just tested, the tabulated validity value was found to be 3.50. It is evident that this value is extremely high in the incorrect matrix range. Hence there is but little doubt that the analytic matrix (key-length of 14) is incorrect.

Let us similarly test the key-length 7. The results are as follows:

1	2	3	4	5	6	7	Number of Vowels	Mean Difference
Ⓤ	R	F	Ⓤ	Ⓞ	P	S	3	.2
R	V	Z	M	L	Ⓔ	L	1	1.8
Ⓘ	Ⓐ	S	Ⓐ	T	Ⓨ	Ⓔ	5	2.2
R	T	S	H	C	L	R	0	2.8
T	Ⓔ	Ⓘ	K	W	Ⓞ	Ⓔ	4	1.2
P	P	T	Ⓘ	V	R	T	1	1.8
Ⓔ	Ⓘ	L	Ⓔ	Ⓐ	Ⓐ	Ⓞ	6	3.2
G	Ⓐ	F	C	W	Ⓔ	M	2	.8
							22 = total vowels	14.0 = total mean differences

22/8=2.8 *expected mean.* 14.0/8=1.80 *validity value of the matrix.*

The tabulated validity value 1.80 is well within the incorrect range and we can therefore conclude that the analytic matrix (key-length of 7), like the analytic matrix for key-length 14, is probably incorrect.

Let us continue our testing, this time testing the possible key-length 8. Results are as follows:

1	2	3	4	5	6	7	8	Number of Vowels	Mean Difference
Ⓤ	G	Ⓘ	T	K	C	Ⓨ	L	3	.1
R	R	Ⓐ	L	Ⓘ	W	L	Ⓔ	3	.1
Ⓘ	V	F	F	Ⓔ	V	Ⓞ	R	3	.1
R	Ⓐ	Z	Ⓤ	C	Ⓐ	R	Ⓔ	4	.9
T	T	S	M	Ⓞ	W	Ⓐ	T	2	1.1
P	Ⓔ	S	Ⓐ	L	P	Ⓔ	Ⓞ	4	.9
Ⓔ	P	Ⓘ	H	T	Ⓔ	S	M	3	.1
								22 = total vowels	3.3 = total mean differences

22/7=3.1 *expected mean.* 3.3/7=0.47 *validity value of the matrix.*

The validity value of the matrix found in this case is well within the valid matrix range[1] and we may therefore conclude that it is quite likely that this analytic matrix (key-length 8) is valid or correct! That is, the validity value of 0.47 as found indicates that the vowels of the message are evenly distributed on the seven rows of the 8×7 matrix. This is of course indicative of a valid matrix.

To complete the record, however, and also to introduce a slight modification in our testing procedure, let us test the last possible key-length (4).

As in the standard testing, the message is written in the form of the analytic matrix and again the vowels are circled.

1	2	3	4
Ⓤ	Ⓘ	K	Ⓨ
R	Ⓐ	Ⓘ	L
Ⓘ	F	Ⓔ	Ⓞ
R	Z	C	R
T	S	Ⓞ	Ⓐ
P	S	L	Ⓔ
Ⓔ	Ⓘ	T	S
G	T	C	L
R	L	W	Ⓔ
V	F	V	R
Ⓐ	Ⓤ	Ⓐ	Ⓔ
T	M	W	T
Ⓔ	Ⓐ	P	Ⓞ
P	H	Ⓔ	M

At this point we come to the slight modification in testing mentioned above. Since the rows are so short, the test made in the normal fashion is not reliable. Therefore, when the rows are short (six letters or less), it is better to combine the rows in pairs. Thus, in the present case we shall combine successive rows in pairs and make the validity test as usual. The result is the following:

---

[1] See page 65 for the interpretation of validity value ranges.

1 2 3 4	Number of Vowels	Mean Difference
Ⓤ Ⓘ K Ⓨ R Ⓐ Ⓘ L	5	1.9
Ⓘ F Ⓔ Ⓞ R Z C R	3	.1
T S Ⓞ Ⓐ P S L Ⓔ	3	.1
Ⓔ Ⓘ T S G T C L	2	1.1
R L W Ⓔ V F V R	1	2.1
Ⓐ Ⓤ Ⓐ Ⓔ T M W T	4	.9
Ⓔ Ⓐ P Ⓞ P H Ⓔ M	4	.9
	22 = total vowels	7.1 = total mean differences

22/7=3.1 *expected mean.* 7.1/7=1.01 *validity value of the matrix.*

The tabulated validity value, 1.01, is high in the indefinite range and therefore is probably incorrect. In fact, since we have already found key-length 7 to be correct, the validity value of 1.01 would have to be incorrect. Note that the total number of vowels (22) is divided in this case by the number of pairs of rows (7) in order to obtain the expected mean. The total of the mean differences is similarly divided by the number of pairs of columns in order to obtain the desired validity value of the matrix.

To summarize, we have made the following four tests of possible size completely filled matrices:

Key-Length	Validity Value of the Matrix
14	3.50
8	0.47
7	1.80
4	1.01

It is easily seen that the key-length 8 with a validity value of 0.47 stands well above the others and therefore most likely is correct.

As a concluding remark concerning the identification of the completely filled matrix, the cryptanalyst should not completely rely upon the validity values obtained to the blindness of everything else. Thus, for example, high frequency bigraphs and trigraphs should be on the same row in a valid analytic matrix, and when making his validity tests the cryptanalyst should keep his eyes open for these. For example, if the letter Q is on a row which lacks a letter U, the cryptanalyst would certainly view the analytic matrix with some suspicion, though such a situation might arise if the column containing the letter Q were the right hand column in the enciphering matrix (in which case the letter U would be on the row beneath the row containing the letter Q).

FIGURE 4

TABLE OF KEY-LENGTHS AND COLUMN-LENGTHS OF COMPLETELY FILLED MATRICES—GIVEN THE MESSAGE-LENGTH

This table covers message-lengths from 15 to 300 letters. The key-lengths considered are from 3 to 25. In reading the expressions to the right of the various message-lengths, the first number of the expression is the *key-length* and the second number is the *column-length.* Thus, for example, in the expression 22×9 (which follows the message-length 198), the *key-length* is 22 and the *column-length* is 9. Many message-lengths may be the result of several sizes of completely filled matrices. These various sizes are listed within the limits above.

15—3×5, 5×3
16—4×4, 8×2
17—
18—3×6, 6×3, 9×2
19—
20—4×5, 5×4, 10×2
21—3×7, 7×3
22—11×2
23—
24—3×8, 4×6, 6×4, 8×3, 12×2
25—5×5
26—13×2
27—3×9, 9×3
28—4×7, 7×4, 14×2
29—
30—3×10, 5×6, 6×5, 10×3, 15×2
31—
32—4×8, 8×4, 16×2
33—3×11, 11×3
34—17×2
35—5×7, 7×5
36—3×12, 4×9, 6×6, 9×4, 12×3, 18×2
37—
38—19×2
39—3×13, 13×3

40—4×10, 5×8, 8×5, 10×4, 20×2
41—
42—3×14, 6×7, 7×6, 14×3, 21×2
43—
44—4×11, 11×4, 22×2
45—3×15, 5×9, 9×5, 15×3
46—23×2
47—
48—3×16, 4×12, 6×8, 8×6, 12×4, 16×3, 24×2
49—7×7
50—5×10, 10×5, 25×2
51—3×17, 17×3
52—4×13, 13×4
53—
54—3×18, 6×9, 9×6, 18×3
55—5×11, 11×5
56—4×14, 7×8, 8×7, 14×4
57—3×19, 19×3
58—
59—
60—3×20, 4×15, 5×12, 6×10, 10×6, 12×5, 15×4, 20×3
61—
62—
63—3×21, 7×9, 9×7, 21×3
64—4×16, 8×8, 16×4
65—5×13, 13×5
66—3×22, 6×11, 11×6, 22×3
67—
68—4×17, 17×4
69—3×23, 23×3
70—5×14, 7×10, 10×7, 14×5
71—
72—3×24, 4×18, 6×12, 8×9, 9×8, 12×6, 18×4, 24×3
73—
74—
75—3×25, 5×15, 15×5, 25×3
76—4×19, 19×4
77—7×11, 11×7
78—3×26, 6×13, 13×6
79—
80—4×20, 5×16, 8×10, 10×8, 16×5, 20×4
81—3×27, 9×9
82—
83—

84—3×28, 4×21, 6×14, 7×12, 12×7, 14×6, 21×4
85—5×17, 17×5
86—
87—3×29
88—4×22, 8×11, 11×8, 22×4
89—
90—3×30, 5×18, 6×15, 9×10, 10×9, 15×6, 18×5
91—7×13, 13×7
92—4×23, 23×4
93—3×31
94—
95—5×19, 19×5
96—3×32, 4×24, 6×16, 8×12, 12×8, 16×6, 24×4
97—
98—7×14, 14×7
99—3×33, 9×11, 11×9
100—4×25, 5×20, 10×10, 20×5, 25×4
101—
102—3×34, 6×17, 17×6
103—
104—4×26, 8×13, 13×8
105—3×35, 5×21, 7×15, 15×7, 21×5
106—
107—
108—3×36, 4×27, 6×18, 9×12, 12×9, 18×6
109—
110—5×22, 10×11, 11×10, 22×5
111—3×37
112—4×28, 7×16, 8×14, 14×8, 16×7
113—
114—3×38, 6×19, 19×6
115—5×23, 23×5
116—4×29
117—3×39, 9×13, 13×9
118—
119—7×17, 17×7
120—3×40, 4×30, 5×24, 6×20, 8×15, 10×12, 15×8, 20×6, 24×5
121—11×11
122—
123—3×41
124—4×31
125—5×25, 25×5
126—3×42, 6×21, 7×18, 9×14, 14×9, 18×7, 21×6
127—

128—4×32, 8×16, 16×8
129—3×43
130—5×26, 10×13, 13×10
131—
132—3×44, 4×33, 6×22, 11×12, 12×11, 22×6
133—7×19, 19×7
134—
135—3×45, 5×27, 9×15, 15×9
136—4×34, 8×17, 17×8
137—
138—3×46, 6×23, 23×6
139—
140—4×35, 5×28, 7×20, 10×14, 14×10, 20×7
141—3×47
142—
143—11×13, 13×11
144—3×48, 4×36, 6×24, 8×18, 9×16, 12×12, 16×9, 18×8, 24×6
145—5×29
146—
147—3×49, 7×21, 21×7
148—4×37
149—
150—3×50, 5×30, 6×25, 10×15, 15×10, 25×6
151—
152—4×38, 8×19, 19×8
153—3×51, 9×17, 17×9
154—7×22, 11×14, 14×11, 22×7
155—5×31
156—3×52, 4×39, 6×26, 12×13, 13×12
157—
158—
159—3×53
160—4×40, 5×32, 8×20, 10×16, 16×10, 20×8
161—7×23, 23×7
162—3×54, 6×27, 9×18, 18×9
163—
164—4×41
165—3×55, 5×33, 11×15, 15×11
166—
167—
168—3×56, 4×42, 6×28, 7×24, 8×21, 12×14, 14×12, 21×8, 24×7
169—13×13
170—5×34, 10×17, 17×10
171—3×57, 9×19, 19×9

172—4×43
173—
174—3×58, 6×29
175—5×35, 7×25, 25×7
176—4×44, 8×22, 11×16, 16×11, 22×8
177—3×59
178—
179—
180—3×60, 4×45, 5×36, 6×30, 9×20, 10×18, 12×15, 15×12, 18×10, 20×9
181—
182—7×26, 13×14, 14×13
183—3×61
184—4×46, 8×23, 23×8
185—5×37
186—3×62, 6×31
187—11×17, 17×11
188—4×47
189—3×63, 7×27, 9×21, 21×9
190—5×38, 10×19, 19×10
191—
192—3×64, 4×48, 6×32, 8×24, 12×16, 16×12, 24×8
193—
194—
195—3×65, 5×39, 13×15, 15×13
196—4×49, 7×28, 14×14
197—
198—3×66, 6×33, 9×22, 11×18, 18×11, 22×9
199—
200—4×50, 5×40, 8×25, 10×20, 20×10, 25×8
201—3×67
202—
203—7×29
204—3×68, 4×51, 6×34, 12×17, 17×12
205—5×41
206—
207—3×69, 9×23, 23×9
208—4×52, 8×26, 13×16, 16×13
209—11×19, 19×11
210—3×70, 5×42, 6×35, 7×30, 10×21, 14×15, 15×14, 21×10
211—
212—4×53
213—3×71
214—
215—5×43

216—3×72, 4×54, 6×36, 8×27, 9×24, 12×18, 18×12, 24×9
217—7×31
218—
219—3×73
220—4×55, 5×44, 10×22, 11×20, 20×11, 22×10
221—13×17, 17×13
222—3×74, 6×37
223—
224—4×56, 7×32, 8×28, 14×16, 16×14
225—3×75, 5×45, 9×25, 15×15, 25×9
226—
227—
228—3×76, 4×57, 6×38, 12×19, 19×12
229—
230—5×46, 10×23, 23×10
231—3×77, 7×33, 11×21, 21×11
232—4×58, 8×29
233—
234—3×78, 6×39, 9×26, 13×18, 18×13
235—5×47
236—4×59
237—3×79
238—7×34, 14×17, 17×14
239—
240—3×80, 4×60, 5×48, 6×40, 8×30, 10×24, 12×20, 15×16, 16×15, 20×12, 24×10
241—
242—11×22, 22×11
243—3×81, 9×27
244—4×61
245—5×49, 7×35
246—3×82, 6×41
247—13×19, 19×13
248—4×62, 8×31
249—3×83
250—5×50, 10×25, 25×10
251—
252—3×84, 4×63, 6×42, 7×36, 9×28, 12×21, 14×18, 18×14, 21×12
253—11×23, 23×11
254—
255—3×85, 5×51, 15×17, 17×15
256—4×64, 8×32, 16×16
257—
258—3×86, 6×43

259—7×37
260—4×65, 5×52, 10×26, 13×20, 20×13
261—3×87, 9×29
262—
263—
264—3×88, 4×66, 6×44, 8×33, 11×24, 12×22, 22×12, 24×11
265—5×53
266—7×38, 14×19, 19×14
267—3×89
268—4×67
269—
270—3×90, 5×54, 6×45, 9×30, 10×27, 15×18, 18×15
271—
272—4×68, 8×34, 16×17, 17×16
273—3×91, 7×39, 13×21, 21×13
274—
275—5×55, 11×25, 25×11
276—3×92, 4×69, 6×46, 12×23, 23×12
277—
278—
279—3×93, 9×31
280—4×70, 5×56, 7×40, 8×35, 10×28, 14×20, 20×14
281—
282—3×94, 6×47
283—
284—4×71
285—3×95, 5×57, 15×19, 19×15
286—11×26, 13×22, 22×13
287—7×41
288—3×96, 4×72, 6×48, 8×36, 9×32, 12×24, 16×18, 18×16, 24×12
289—17×17
290—5×58, 10×29
291—3×97
292—4×73
293—
294—3×98, 6×49, 7×42, 14×21, 21×14
295—5×59
296—4×74, 8×37
297—3×99, 9×33, 11×27
298—
299—13×23, 23×13
300—3×100, 4×75, 5×60, 6×50, 10×30, 12×25, 15×20, 20×15, 25×12

Problems

Each of the following messages has been enciphered with a completely filled matrix.

31. AHHGL TLSGB WTCSN TNAEU YWIYE
ETOMR WEREI SOTDE NAEEA OLIAS
DNSPE XENHF PIINE EHONE HATCA
GSINS MRTDA KTD

32. INNYC OTSDN SOULW PEBOO PTEGN
EMRAE PRULD SOALT MLTTP TBOTR
IYIID HOIBO UNOXC IEKTR LOTFA
ERNAA OWHOS AIHAU NBTTI P

33. ADIUO SNAPO RIRAN DMPEE CLTBA
NOLES RLFOM ERETT FEETN DISLP
ATPLT WANEA IWADE EYGMN

34. PCYCY NFNSO HOASE UVLEA WIMIE
IIRNN NAENI SREED ERRGN TNKEB
ALRNR IRTUS EIASG IEMRI GD

35. NPLRM GOFAT RRHRT BEEGD SCENT
ECEPO TIAAD LFEYE MOPSN MSCAT
USETY TNLIH ELOOB TTIEU ONONI
IOIAS CVGFD RCOPP P

36. NIOSX NWEVN VELWR CTSTB LNIJF
CWNIN OOAWE IEDXE TITII THEVL
INPTI DTRAI PINAI CEDLE EYITO
HYCYF HSRRL TEIYT AOFRT EUAUN
UITIT ROGIU DS

37. IAOEP PISTY IUPUS LSOTT SLGHP
IIBOE RTLON IDHST LSPES KNIEH
ETWOO AUEHV KDEFB ONANE ANTIW
RLPRP EIWRE AUEMD ATSWG SOBQC
GAAAD EMNIE SISUE NUTNL SRSLN
ERCKW SSORP OLLIM

38. SAIWN ANIMT AESOE YSNPS LOUCT
NEEIW HSRBT TRLSO SSBJE UOHDL
GTIEL RSPPA OAOIE E

39. URBRI ROEPD ESANS TASAM INOTR
DAMEG YFRAE DTSDL ETWOS FGTOT
TSBEN EEEOE NMUAM BASII PEASF
ANNLE XNTEE RCETI LUEXE OLKDE
NNRPI DSV

40. CKIAC ESAIA NOLVR ANOSM TEEEC
DLCTH SWSSU MKECV RDIBN STPTE
ELUPT APSIA OEYEM SEEHO MSORR
HNSNR SLOTL LAFIT

Chapter XII

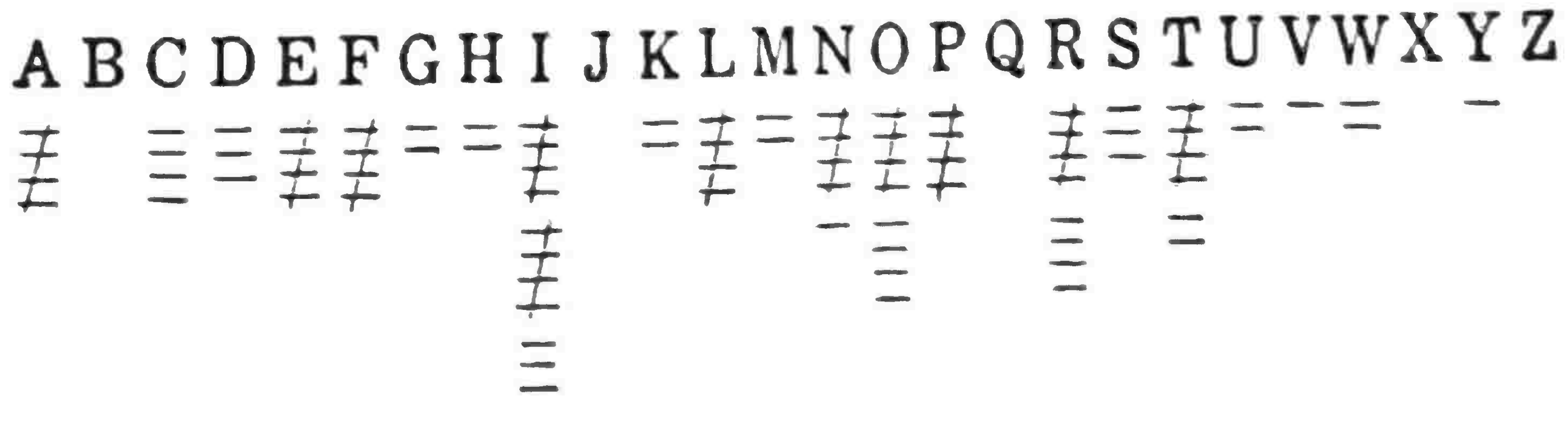
Cryptanalytic Solution

Given: The Key-length plus a Probable Word in the Text.

The problem of solving a single columnar transposition cipher, given the key-length and a probable word in the text, is relatively simple. Given the key-length, which in itself is possibly ninety-percent of the solution, allows the cryptanalyst to mechanically construct the analytic matrix; and the analytical juxtapositioning of the matrix columns is then facilitated greatly by the given probable word. Let us go through the steps in the solution of an actual example. We are given the following cipher-text message together with the key-length 9 plus the probable word NEW YORK:

RCRKA LPTNA TALMO IDFNV TRTIN
FLEFR IONOI WOPIE CGOAF RDCUH
OIAIT ELLPR IRPSN EYRRC IHITI
OTWUO IDSPF SOIEK GMN

The monoliteral frequency distribution of the message is easily tabulated as follows:



Given the key-length 9, construction of the analytic matrix[1] is routine:

---

[1] See Chapter VIII.

```
    T I C O I
  T R O G I R H
R A T|N O A P I S
C L I O A I S T P
R M N I F T N I F
K O F W R E E O S
A I L O D L Y T O
L D E P C L R W I
P F F I U P R U E
T N R E H R C O K
N V I C O I I I G
A T O G I R H D M
T R N O A P I S N
```

The cryptanalyst's task now is to rearrange these nine columns to yield the plain-text message. To do this the cryptanalyst uses the probably word NEW YORK. Examination of the monoliteral frequency distribution shows that the letters of the probable word NEW YORK occurred with the following frequencies:

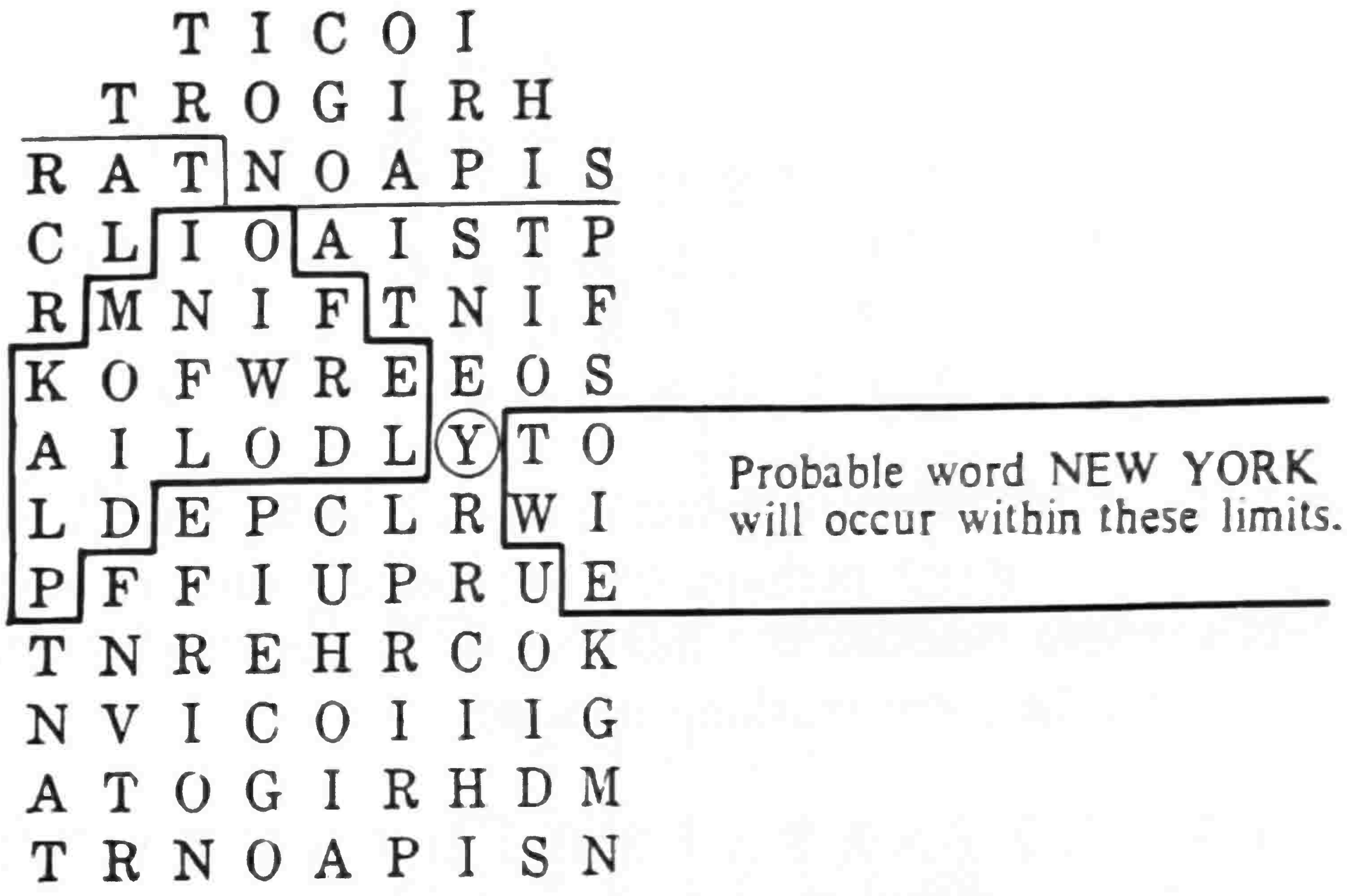
```
            N E W Y O R K
frequency = 6 5 2 1 9 9 2
```

The letters in which we are most interested are *those letters which are most easily identifiable in the cipher-text message.* The letter Y with a frequency of 1 is of course the ideal situation, for the one letter Y in the message must be the letter Y in our given probable word! The letter Y in the analytic matrix is found and circled:

```
    T I C O I
  T R O G I R H
R A T|N O A P I S
C L I O A I S T P
R M N I F T N I F
K O F W R E E O S
A I L O D L Ⓨ T O
L D E P C L R W I
P F F I U P R U E
T N R E H R C O K
N V I C O I I I G
A T O G I R H D M
T R N O A P I S N
```

By identifying the letter Y in the analytic matrix we are able to narrow down considerably the location within the columns of the remaining letters of the probable word NEW YORK.

Thus, the remaining letters of the probable word NEW YORK must occur within the following limits:



```
    T I C O I
  T R O G I R H
R A T N O A P I S
C L I O A I S T P
R M N I F T N I F
K O F W R E E O S
A I L O D L Y T O
L D E P C L R W I
P F F I U P R U E
T N R E H R C O K
N V I C O I I I G
A T O G I R H D M
T R N O A P I S N
```

Probable word NEW YORK will occur within these limits.

How these limits within the columns are obtained is very important. There are several somewhat mechanical methods for obtaining these limits. The following is one of these:

As we remember from the construction of the analytic matrix,[1] below the matrix cap the cipher-text message is written in successive columns from left to right. In marking off the limitations or limits we treat the columns (staying below the matrix cap) just as if the message were written out horizontally. Thus we start at the given known letter—in this case the letter Y—and mark off both forward and backward first the number of long column lengths—in this case three column lengths of 11—and then the remaining short column lengths— in this case column lengths of 10—until the entire matrix is marked off. The analytic matrix at this point will look as follows:

---

[1] See Chapter VIII.

$$\begin{array}{ccccccccc}
 & & T & I & C & O & I & & \\
 & T & R & O & G & I & R & H & \\
\overline{R} & \overline{A} & \overline{T}\,| & \underline{N} & \underline{O} & \underline{A} & \underline{P} & \underline{I} & \underline{S} \\
C & L & \overline{I} & \overline{O} & A & I & S & T & P \\
R & \overline{M} & N & I & \overline{F} & T & N & I & F \\
\overline{K} & O & F & W & R & \overline{E} & E & O & S \\
A & I & L & O & D & L & \textcircled{Y} & T & O \\
L & D & E & P & C & L & R & W & I \\
P & F & F & I & U & P & R & \overline{U} & E \\
T & N & R & E & H & R & C & O & \overline{K} \\
N & V & I & C & O & I & I & I & G \\
A & T & O & G & I & R & H & D & M \\
T & R & N & O & A & P & I & S & N
\end{array}$$

This marking off of long columns and then short columns within the analytic matrix might perhaps be more easily understood if the cipher-text message beneath the matrix cap is actually written out horizontally and the same marking is done:

```
    R C R/K A L P T N A T A L/M O I D F N V T R T/I N
         <---------10---------> <---------10--------> <---
    F L E F R I O N/O I W O P I E C G O A/F R D C U H
 ---------10--------> <---------11---------> <------11---
    O I A I T/E L L P R I R P S N E(Y)R R C I H I T I
 -------------> <---------11---------> <--------11-------
    O T W/U O I D S P F S O I E/K G M N
 --------> <-----------11--------->
```

Compare this marking off with the marking off within the analytic matrix above.

The next step in our marking off of the limits within the columns may seemingly be a little complicated but actually it isn't as complicated as it seems. Using the analytic matrix cap as a guide we obtain a series of numbers, in this case 2 3 4 4 4 4 3 2. These numbers are obtained from the "cap" as follows:

```
  2 3 4 4 4 4 3 2
      T I C O I
    T R O G I R H
  R A T|N O A P I S
  . . . O A I S T P
  . . . . . . . . .
```

Note that in obtaining this series of numbers from right to left we count the number of letters in each column *including one letter beneath the cap!*

With these series of numbers we mark off the ends of the already marked off columns. In the horizontal message this marking off of the ends will appear as follows:

$$\text{R C R/K A }\overset{4}{\text{L}}\text{ P/T N A T A L/M O }\overset{4}{\text{I}}\text{ D/F N V T R T/I }\overset{4}{\text{N}}$$

$$\text{F L/E F R I O N/O }\overset{4}{\text{I}}\text{ W O/P I E C G O A/F }\overset{3}{\text{R}}\text{ D/C U H}$$

$$\text{O I A I T/E }\overset{2}{\text{L}}\text{ L/L P R I R P S N E }\text{\textcircled{Y}}\text{ R R C I H I T I}$$

$$\text{O/T }\overset{2}{\text{W}}\text{/U O I D S P F S/O }\overset{3}{\text{I}}\text{ E/K G M N}$$

And the analytic matrix with the marked off "ends" is as follows:

$$\begin{array}{ccccccccc}
 & & \mathrm{T} & \mathrm{I} & \mathrm{C} & \mathrm{O} & \mathrm{I} & & \\
 & \mathrm{T} & \mathrm{R} & \mathrm{O} & \mathrm{G} & \mathrm{I} & \mathrm{R} & \mathrm{H} & \\
\cline{1-3}
\mathrm{R} & \mathrm{A} & \multicolumn{1}{c|}{\underline{\mathrm{T}}} & \mathrm{N} & \mathrm{O} & \mathrm{A} & \mathrm{P} & \mathrm{I} & \mathrm{S} \\
\cline{4-9}
\mathrm{C} & \underline{\mathrm{L}} & \mathrm{I} & \mathrm{O} & \underline{\mathrm{A}} & \mathrm{I} & \mathrm{S} & \mathrm{T} & \mathrm{P} \\
\underline{\mathrm{R}} & \mathrm{M} & \mathrm{N} & \mathrm{I} & \mathrm{F} & \underline{\mathrm{T}} & \mathrm{N} & \mathrm{I} & \mathrm{F} \\
\mathrm{K} & \mathrm{O} & \mathrm{F} & \mathrm{W} & \mathrm{R} & \mathrm{E} & \mathrm{E} & \underline{\mathrm{O}} & \underline{\mathrm{S}} \\
\mathrm{A} & \mathrm{I} & \underline{\mathrm{L}} & \underline{\mathrm{O}} & \underline{\mathrm{D}} & \underline{\mathrm{L}} & \text{\textcircled{Y}} & \mathrm{T} & \mathrm{O} \\
\mathrm{L} & \underline{\mathrm{D}} & \mathrm{E} & \mathrm{P} & \mathrm{C} & \mathrm{L} & \mathrm{R} & \underline{\mathrm{W}} & \mathrm{I} \\
\underline{\mathrm{P}} & \mathrm{F} & \mathrm{F} & \mathrm{I} & \mathrm{U} & \mathrm{P} & \mathrm{R} & \mathrm{U} & \underline{\mathrm{E}} \\
\mathrm{T} & \mathrm{N} & \mathrm{R} & \mathrm{E} & \mathrm{H} & \mathrm{R} & \mathrm{C} & \mathrm{O} & \mathrm{K} \\
\mathrm{N} & \mathrm{V} & \mathrm{I} & \mathrm{C} & \mathrm{O} & \mathrm{I} & \mathrm{I} & \mathrm{I} & \mathrm{G} \\
\mathrm{A} & \mathrm{T} & \mathrm{O} & \mathrm{G} & \mathrm{I} & \mathrm{R} & \mathrm{H} & \mathrm{D} & \mathrm{M} \\
\mathrm{T} & \mathrm{R} & \mathrm{N} & \mathrm{O} & \mathrm{A} & \mathrm{P} & \mathrm{I} & \mathrm{S} & \mathrm{N}
\end{array}$$

The limits of the letters of the probably word NEW YORK are these "ends" of the marked off columns. It should be noted that the use of the series of numbers, in this case 2 3 4 4 4 4 3 2, is only a method of convenience to obtain the desired limitations within the respective columns. The same result is obtained, if instead of using the series of numbers, you simply mark off new columns—going away from the letter Y—with first the six short columns (of length 10) and then finishing up with the long columns. This is the reverse of our first step above when we marked off first the long columns and then the short columns.

We shall return to the "theory" behind this limitation of columns later; however, for now let us continue the solution of our given message. We now have the following analytic matrix:

1	2	3	4	5	6	7	8	9
		T	I	C	O	I		
	T	R	O	G	I	R	H	
R	A	T	N	O	A	P	I	S
C	L	I	O	A	I	S	T	P
R	M	N	I	F	T	N	I	F
K	O	F	W	R	E	E	O	S
A	I	L	O	D	L	Ⓨ	T	O
L	D	E	P	C	L	R	W	I
P	F	F	I	U	P	R	U	E
T	N	R	E	H	R	C	O	K
N	V	I	C	O	I	I	I	G
A	T	O	G	I	R	H	D	M
T	R	N	O	A	P	I	S	N

Probable word NEW YORK will occur within these limits.

Since the letter Y occurs in column 7 we have the following beginning for the juxtaposition or reconstruction of columns in the enciphering matrix:

7
I
R
P
S
N
E
N E W Y O R K
R
R
C
I
H
I

Examination of the columns of the analytic matrix shows that there is but one letter K within the given limits of the columns. This is the letter K in column 1. Therefore, we may add column 1 to our juxtaposition:

```
      7     1
      -     -
      I
      R
      P
      S     R
      N     C
      E     R
N E W Y O R K
-------------
      R     A
      R     L
      C     P
      I     T
      H     N
      I     A
            T
```

In a similar manner, the letter N can come only from column 3:

```
3     7     1
-     -     -
      I
      R
T     P
R     S     R
T     N     C
I     E     R
N E W Y O R K
-------------
F     R     A
L     R     L
E     C     P
F     I     T
R     H     N
I     I     A
O           T
N
```

The letter R can come only from column 5, and another column may be added:

3			7		5	1
			I			
			R		C	
T			P		G	
R			S		O	R
T			N		A	C
I			E		F	R
N	E	W	Y	O	R	K
F			R		D	A
L			R		C	L
E			C		U	P
F			I		H	T
R			H		O	N
I			I		I	A
O					A	T
N						

In the juxtaposition of column 5 with column 1, note the high-frequency bigraphs which result. These "good" bigraphs confirm the validity of our analysis to this point.

At this point solution is practically guaranteed. With the already recovered bigraphs, plus the word NEW YORK, and the limitations within the columns of the letters NEW YORK, solution is routine. For example, the letter E of NEW YORK can only come from either column 6 or 9, etc. At this point we shall end our solution. However, the student for his own benefit should finish the complete solution.

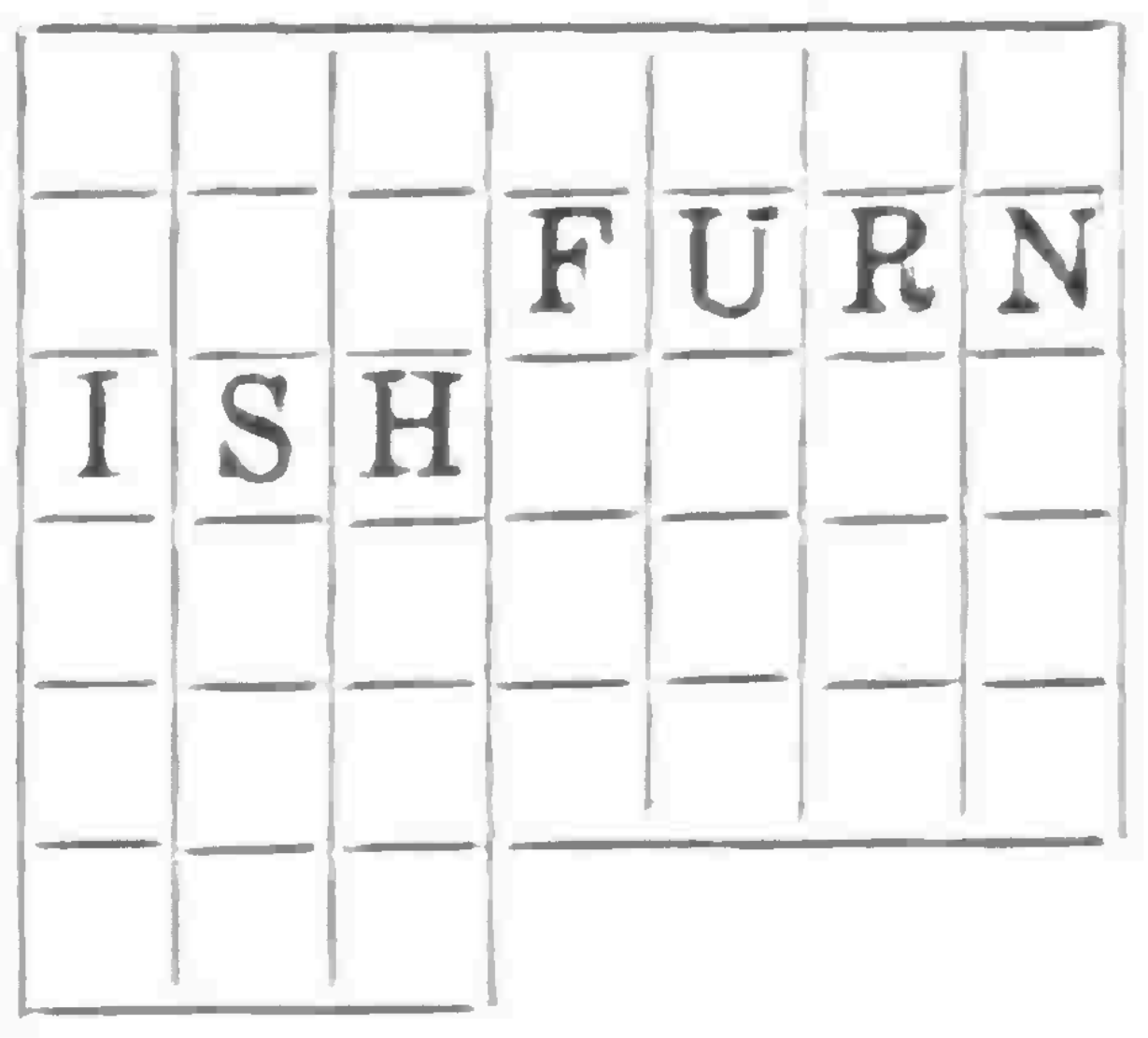
We mentioned earlier in this chapter that we would return to the theory behind the limitations within columns. Because of the importance of this particular phase of solution, we shall finish this chapter with a few final remarks regarding this "theory."

Note the following enciphering matrix with consideration given only to the letters on one line:

F	U	R	N	I	S	H

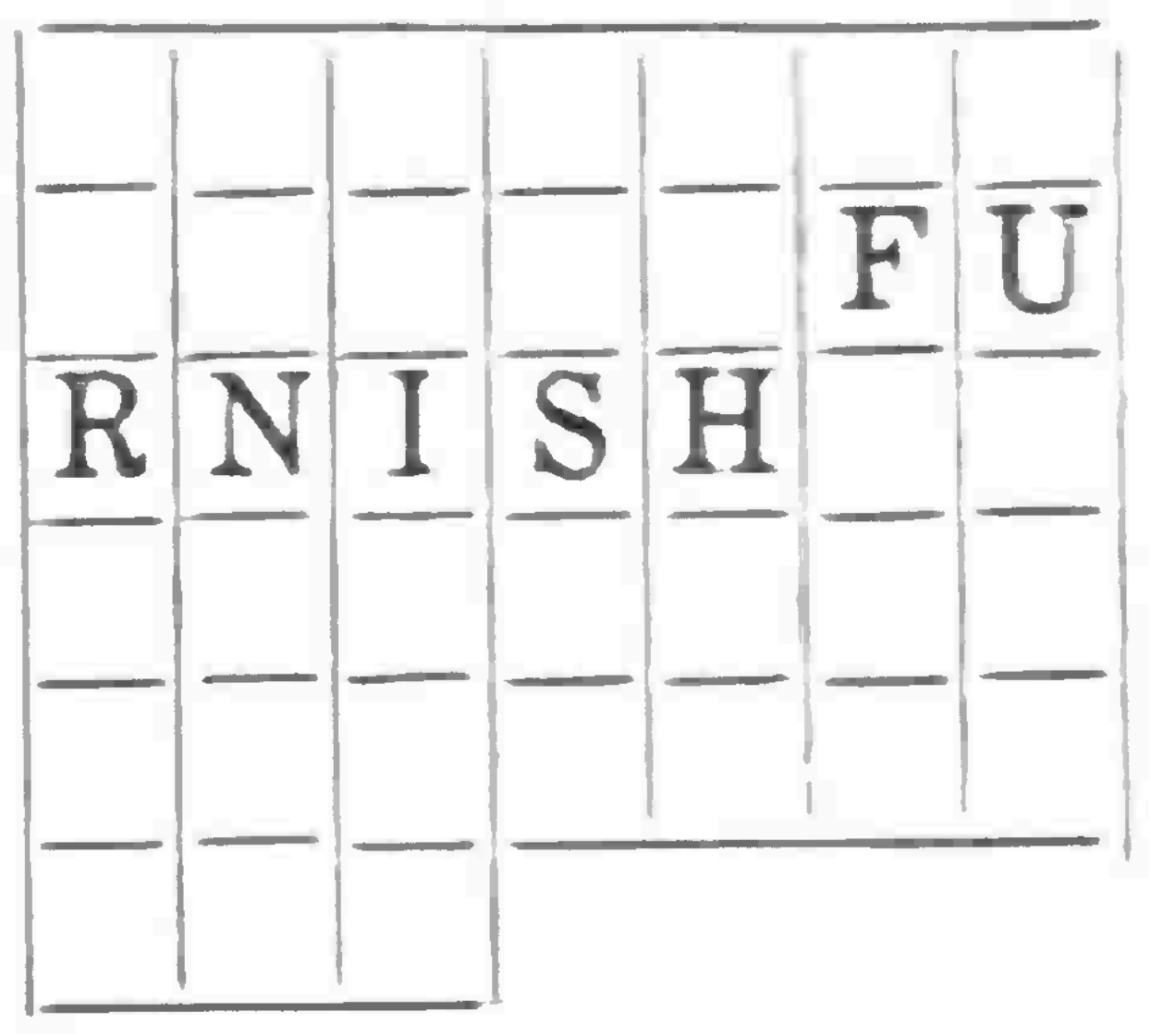
It may be seen that the *literal* distance from one letter to another will always be either a long column length or a short column length.

Consider the same letters in the matrix as follows:



Note again that the distance between any two letters is a column length—and in this particular case, more specifically, the distance is a short column length.

But consider now the following:



Here we see an exception! The distance between the letters S or H and F or U is one less than a short column length.

Having looked at these enciphering matrices containing the word FURNISH, we arrive at an important fact: Except for the last exception above, successive letters of plain-text not longer than the key-length (as the word FURNISH above for example) in the final cipher-text message will be separated by a multiple of long and short columns. Even the exception does not apply *unless the number of successive plain-text letters is at least two letters longer than the number of long columns in the enciphering matrix.*

It should be realized that the important fact of successive letters being separated in the final cipher-text by a multiple of column lengths was the basis for obtaining the limits within columns of the letters of the probable word NEW YORK—as was done somewhat mechanically earlier in this chapter.

When those limitations were found, the letter Y was used as the "basic" letter. Since there were only three letters to the left of the letter Y (NEW), and only three letters to the right of the letter Y

(ORK), the exception above was not applicable (since the number of long columns in the matrix was 3). However, if the "basic" letter had been the letter N (instead of Y), the exception would have been applicable and the letters ORK might have occurred outside the limitations. This exception is perhaps an improbability, but the student should be aware of its possibility.

Problems

41. Given the key-length of 8 and the probable word EXTRACT.

```
OIICN ISLSN TEOOE DYSCE WIRLF
NEWEO DTSHS FGTAM TPIAI XEWRX
FOSKC ONENA ROKOW EOEWL NOTEM
TLETT KIMTR RTSRP NE
```

42. Given the key-length 16 and the probable word UTILIZED.

```
WEPRE IBLOH LEDAA DOBIM FTREN
LLRAI RSTSC ICETL AHOZE REETE
IULID CEEPT TAVSU MPALL ENAUE
CDUST TOEAC IIVUP MCIRD TMSFR
RLSNH HORDF AENOS FOTOW TAEPT
UFSBE RTTTE T
```

43. Given the key-length 16 and the probable word MEXICO CITY.

```
UTAND ZTWPO TOAER GSPCS EFXRP
OARAM AOLEO LNEIE ARCAF POERE
NMCTR RHYOT CIONS YMIER CSISA
IAOYR LSIOI LOSQY OOTEN OVUSF
ICERS ECIMO BMCAA HLNVI OOCOE
UDUEA UYNYD ERKBE XNECN SETFI
TSEYH
```

44. Given the key-length 9 and the probable word KEY WEST.

```
UIKUI MANIS SFYFR OITRE EEITU
TIDSN SOAIB GENEA SVNMH YIDNT
EGEFB IECDA NOTTH PRGAT WDFSG
S
```

45. Given the key-length 12 and the probable word TWELVE.

```
WEWNM DJOLT ZWENC CAOST OASKC
TOERD ILZEE RAETP EUECT VIAOT
BIANA LRRPO HIAKO HEOWD TEZOS
PIITE RLSTN AROVT ET
```

46. Given the key-length 10 and the probable word REQUEST.

EJHOO IABDL TMENJ TSICU NPKKT
ODEEE WSOHN ERSSH INSDL SATTW
EDLRD HEIEN PIEEQ OICRX MEPET
ENNUO WVHRT SDYSI LEU

47. Given the key-length 11 and the probable word TWELVE.

MOLMX RNERT VATHE HNWCN OTEFI
EONBN TTNTH EINIO EUPUL ITSAM
ONLRC EGW

48. Given the key-length 10 and the probable word STOP.

SEFRF RBOLI HLWOH RNSOE EEFET
ACTPE HAEIN ELPNT OSDLF CAOEN

49. Given the key-length 10 and the probable word STRIKE.

NNNRS IKOCI TPOEL NOORN PITPE
TICSC EPORA OTTAW UTOIP FDLFA
TNOSR IINTE GEKOY DCGAI SRSEM
ESUOT MER

50. Given the key-length 6 and the probable word WILL.

EQNBI YETHA MLRDO EXXUT ESORY
RPIUE TWITI WFHCT SEELN BBNT

Chapter XIII

Cryptanalytic Solution

Given: A Probable Word in the Text.

The last chapter discussed the cryptanalytic solution of the single columnar transposition cipher given a probable word in the text plus the key-length. In this chapter we shall now consider the same problem except that this time we shall not know the key-length.

Since there are but a limited number of possible key-lengths, it is obvious that merely by trial-and-error we might reduce the problem in this chapter to the same problem whose solution was taken up in the last chapter. This is, we might simply try key-length after key-length until we finally hit the one which leads to solution. At first this might seem a tedious task. However, depending upon the particular cipher-text message involved plus the known "probable word", this trial-and-error testing can often be done fairly rapidly. Consider for example the following cryptogram where we are given the probable word ACKNOWLEDGE:

EERAN SIEOO YDYSL PEECL TETIV
OCPTT REOUR WAOOE TDIEE TEFTI
OOESN AWTRS SNYWF TRCLS URSSE
MHAKE DDUAY GSPRY MBSCF PCSEQ
OTORD SIEHL IERRY EECIG NPEDP
TRKPE HNOCE ALSNT BSROO BKJAE
A

As a first step in solution we construct a biliteral frequency distribution of the message:

A—NOWKYLE
B—SSK
C—LPLFSIE
D—YIDUSP
E—EROECTOTETFSMDQHRECDHAA
F—TTP
G—SN

H—A L N
I—E V E O E E G
J—A
K—E P J
L—P T S I S
M—H B
N—S A Y P O T
O—O Y C U O E O E T R C O B
P—E T R C E T E
Q—O
R—A E W S C S Y D R Y K O
S—I L N S N U S E P C E I N R
T—E I T R D E I R R O R B
U—R R A
V—O
W—A T F
X—
Y—D S W G M E
Z—

One important thing is immediately noted—the text contains the letter Q. How this may provide a major wedge towards solution will be seen later. For now let's consider what the minimum key-length might be. Since we are provided with the probable word ACKNOWLEDGE we can use the same technique as described in Chapter VII to determine whether or not the given probable word is longer than the key-length. If the probable word is longer than the key-length, solution will of course be greatly simplified. Thus, following the procedure of Chapter VII, using the given probable word ACKNOWLEDGE and the biliteral frequency distribution, we obtain the following:

A	C	K	N	O	W
C	K	N	Ⓞ	W	L
Ⓚ	N	O	W	L	E
Ⓝ	O	W	L	Ⓔ	D
Ⓞ	W	L	E	D	G
Ⓦ	Ⓛ	Ⓔ	D	G	E
Ⓛ	Ⓔ	D	G	Ⓔ	
Ⓔ	D	G	E		
D	G	Ⓔ			
G	Ⓔ				
Ⓔ					

Provided that the probable word ACKNOWLEDGE is valid, from the above diagram it is seen that the minimum possible good key-length is 10. In this case the last letter E of ACKNOWLEDGE will fall under the first letter A as follows:

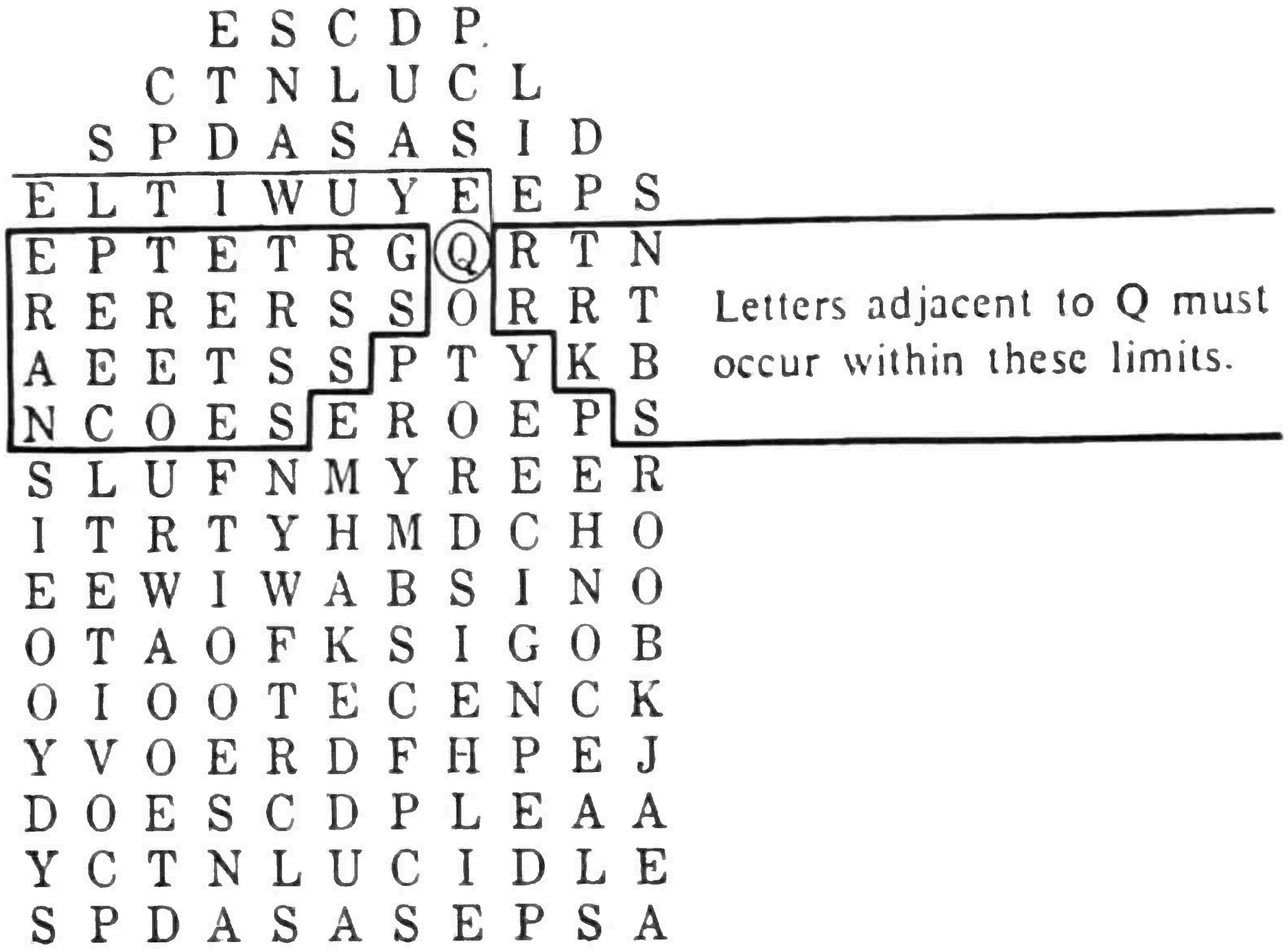
```
A C K N O W L E D G
E
```

Therefore, let us begin our trial-and-error testing of key-lengths by beginning with the key-length 10. Since we are fortunate to have a letter Q in the message, we can use the fact that the letter Q is normally followed by the letter U as a test for the initial validity of the constructed analytic matrix. That is, for the key-length 10 we shall first construct the analytic matrix, then using Q as the "basic letter" we shall determine the limits of adjacent letters. We thus arrive at the following:

```
   Key-Length 10
E P R T S M M S N A
E E E E N H B I P L
R E O F Y A S E E S
A C U T W K C H D N
N L R I F E F L P T
S T W O T D P I T B
I E A O R D C E R S
E T O E C U S R K R
O I O S L A E R P O
O V E N S Y Q Y E O   Letters adjacent to Q must
Y O T A U G O E H B   occur within these limits.
D C D W R S T E N K
Y P I T S P O C O J
S T E R S R R I C A
L T E S E Y D G E E
P R T S M M S N A A
```

Since it is evident that there is no letter U within the limits of the letters adjacent to the letter Q, the key-length 10 may be considered as in-valid and we may proceed to the next possible key-length 11:

Key-Length 11

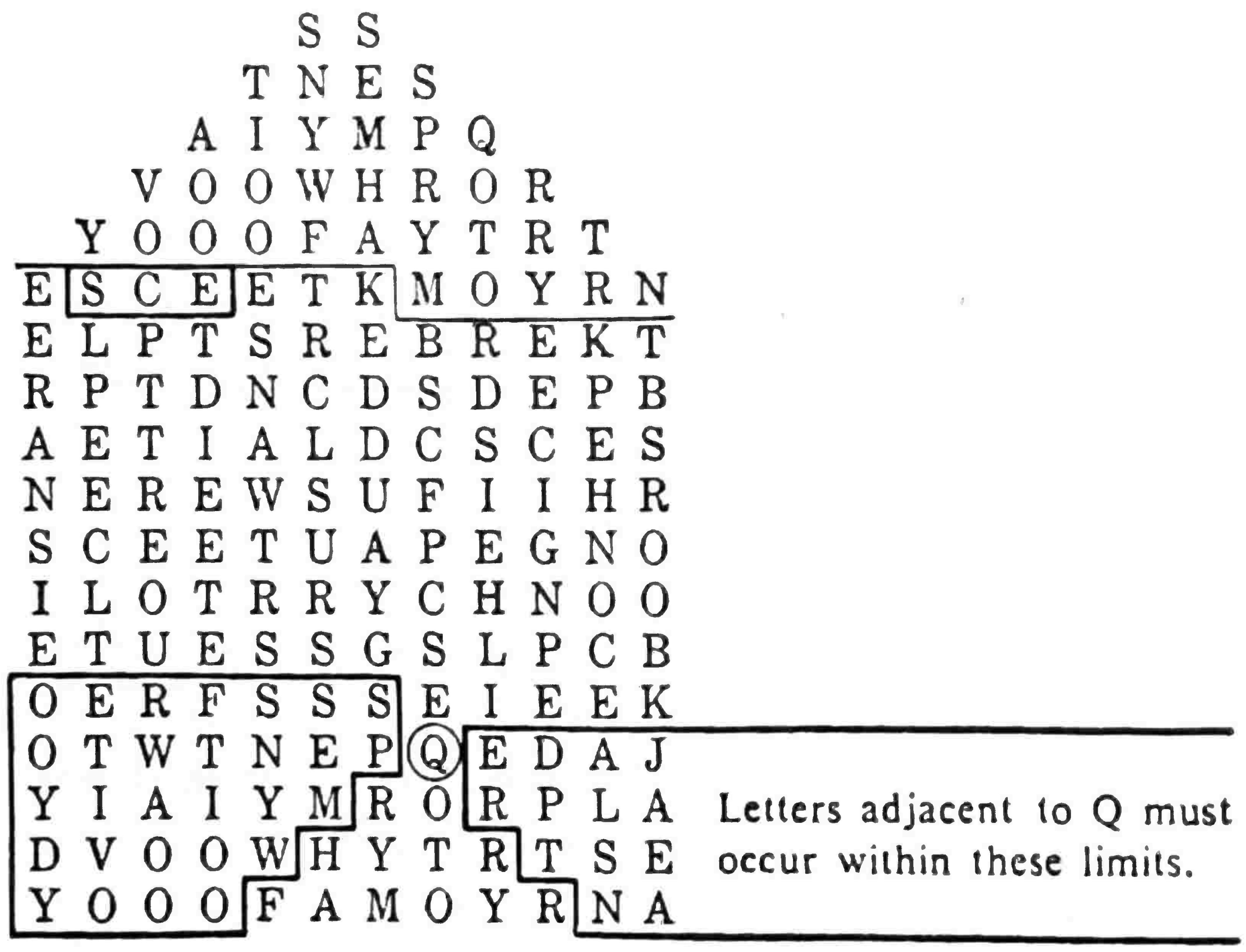


```
         E S C D P.
       C T N L U C L
     S P D A S A S I D
E L T I W U Y E E P S
E P T E T R G Q R T N
R E R E R S S O R R T
A E E T S S P T Y K B
N C O E S E R O E P S
S L U F N M Y R E E R
I T R T Y H M D C H O
E E W I W A B S I N O
O T A O F K S I G O B
O I O O T E C E N C K
Y V O E R D F H P E J
D O E S C D P L E A A
Y C T N L U C I D L E
S P D A S A S E P S A
```

Letters adjacent to Q must occur within these limits.

Again there is no letter U within the limits obtained for adjacent letters to "basic letter" Q. Key-length 11 may thus also be discarded. We proceed to key-length 12:

Key-Length 12

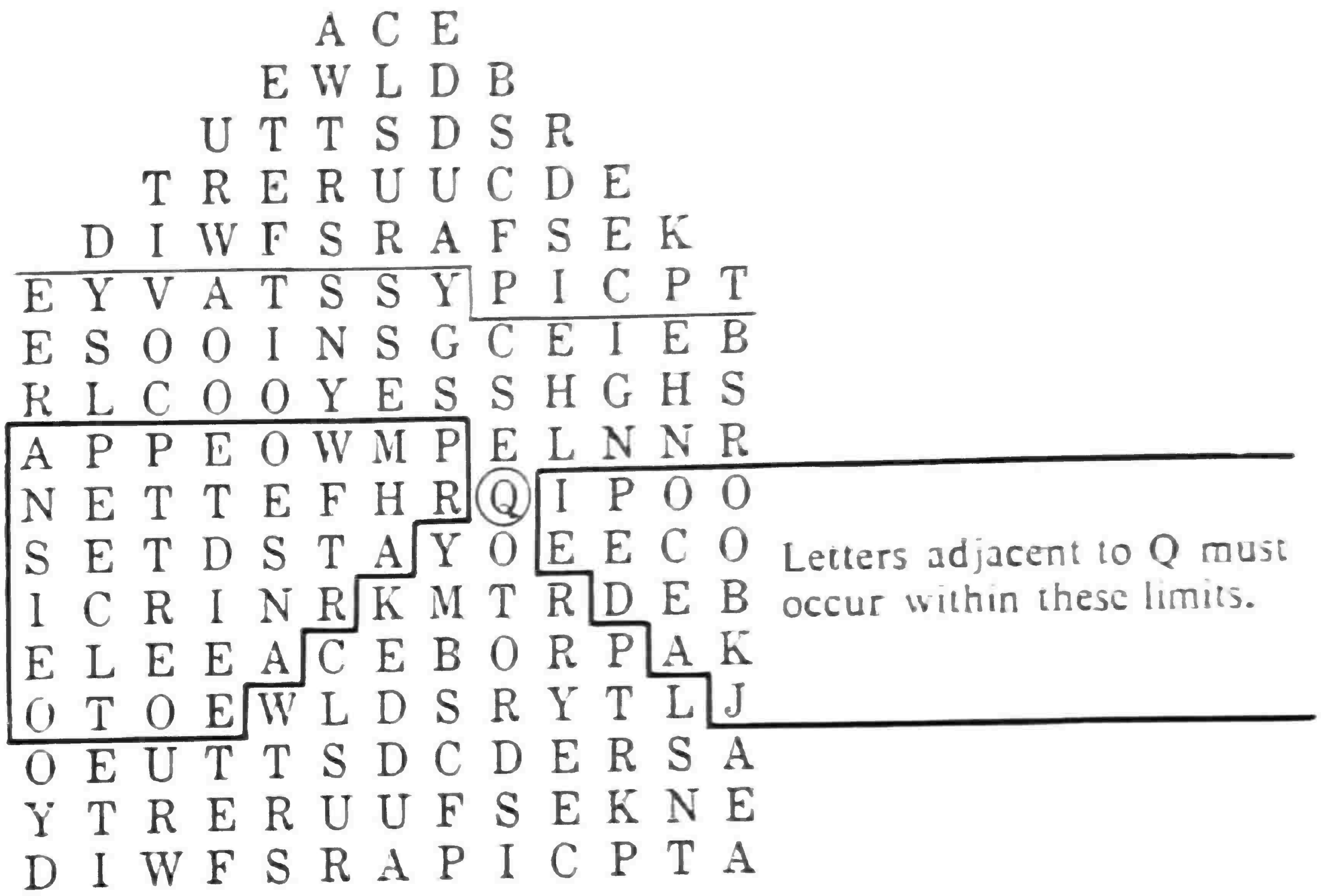


```
          S S
        T N E S
      A I Y M P Q
    V O O W H R O R
  Y O O O F A Y T R T
E S C E E T K M O Y R N
E L P T S R E B R E K T
R P T D N C D S D E P B
A E T I A L D C S C E S
N E R E W S U F I I H R
S C E E T U A P E G N O
I L O T R R Y C H N O O
E T U E S S G S L P C B
O E R F S S S E I E E K
O T W T N E P Q E D A J
Y I A I Y M R O R P L A
D V O O W H Y T R T S E
Y O O O F A M O Y R N A
```

Letters adjacent to Q must occur within these limits.

No letter U occurs within the limits obtained and therefore the key-length 12 may also be discarded. We continue with key-length 13:

Key-Length 13

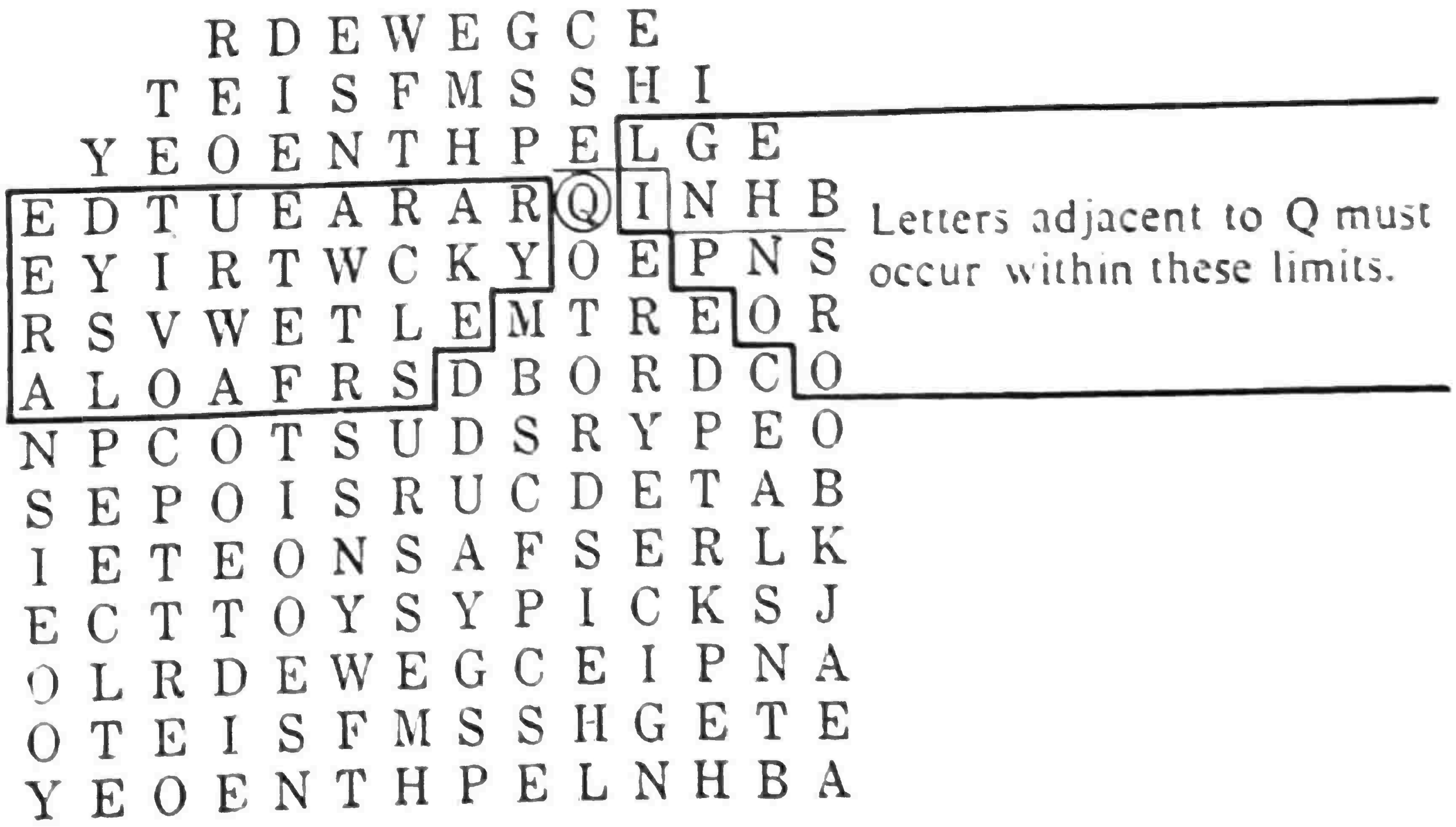


```
          A C E
        E W L D B
      U T T S D S R
    T R E R U U C D E
  D I W F S R A F S E K
E Y V A T S S Y P I C P T
E S O O I N S G C E I E B
R L C O O Y E S S H G H S
A P P E O W M P E L N N R
N E T T E F H R Q I P O O
S E T D S T A Y O E E C O
I C R I N R K M T R D E B
E L E E A C E B O R P A K
O T O E W L D S R Y T L J
O E U T T S D C D E R S A
Y T R E R U U F S E K N E
D I W F S R A P I C P T A
```

Letters adjacent to Q must occur within these limits.

Once again no letter U occurs within the limits obtained and therefore the key-length 13 may be discarded. We turn to key-length 14:

Key-Length 14



```
      R D E W E G C E
    T E I S F M S S H I
  Y E O E N T H P E L G E
E D T U E A R A R Q I N H B
E Y I R T W C K Y O E P N S
R S V W E T L E M T R E O R
A L O A F R S D B O R D C O
N P C O T S U D S R Y P E O
S E P O I S R U C D E T A B
I E T E O N S A F S E R L K
E C T T O Y S Y P I C K S J
O L R D E W E G C E I P N A
O T E I S F M S S H G E T E
Y E O E N T H P E L N H B A
```

Letters adjacent to Q must occur within these limits.

At last! A letter U occurs within the obtained limits. Let us juxtapose column 10, containing the letter Q, in front of column 4, containing the letter U, thus putting the Q U together as follows:

10	4
C	R
S	E
E	O
Q	U
O	R
T	W
O	A
R	O
D	O
S	E
I	T
E	D
H	I
L	E

Visually the bigraphs look excellent! It is likely that with the key-length of 14 we have finally hit the correct key-length. How can we now use our probable word ACKNOWLEDGE at this point? If these two columns are correctly juxtaposed, it is likely that the word ACKNOWLEDGE has at some point crossed these two columns. We can look therefore within these juxtaposed columns for bigraphs formed from successive letters of the probable word ACKNOWLEDGE. That is, in the two juxtaposed columns above we can look for any of the following bigraphs:

A C
C K
K N
N O
O W
W L
L E
E D
D G
G E

In the two juxtaposed columns we find two such bigraphs:

10	4	
C	R	
S	E	
E	O	
Q	U	
O	R	
T	W	
O	A	
R	O	
D	O	
S	E	
I	T	
E	D	/
H	I	
L	E	/

If the bigraph LE is correctly from the word ACKNOWLEDGE, it will be followed by the letter D—which letter should be on the bottom of the constructed analytic matrix. However, there is no letter D on or close to the bottom of the analytic matrix. Therefore, we may conclude that the bigraph LE is not from the word ACKNEWLEDGE. Consider however the bigraph ED. If ED correctly comes from the word ACKNOWLEDGE, it will be followed by the letter G. Sure enough, there is such a G in column 8. Therefore, let us juxtapose column 8 against the two already juxtaposed columns.

	10	4	8	
	C	R	E	
	S	E	M	
	E	O	H	
	Q	U	A	
	O	R	K	
	T	W	E	
	O	A	D	
	R	O	D	
	D	O	U	
	S	E	A	
	I	T	Y	
(ACKNOWL)	E	D	G	(E)
	H	I	S	
	L	E	P	

Juxtaposed column 8 looks excellent together with columns 10 and 4, and there is little doubt but that we now have finally hit pay dirt. Using the letter E from column 10 as the "basic letter" let us see where the remaining letters from the probable word ACKNOWLEDGE can be found.

```
 1  2  3  4  5  6  7  8  9 10 11 12 13 14
-----------------------------------------
          R  D  E  W  E  G  C  E
       T  E  I  S  F  M  S  S  H  I
    Y  E  O  E  N  T  H  P  E  L  G  E
 E  D  T  U  E  A  R  A  R  Q  I  N  H  B
 E  Y  I  R  T  W  C  K  Y  O  E  P  N  S
 R  S  V  W  E  T  L  E  M  T  R  E  O  R
 A  L  O  A  F  R  S  D  B  O  R  D  C  O
 N  P  C  O  T  S  U  D  S  R  Y  P  E  O
 S  E  P  O  I  S  R  U  C  D  E  T  A  B
 I  E  T  E  O  N  S  A  F  S  E  R  L  K
 E  C  T  T  O  Y  S  Y  P  I  C  K  S  J
 O  L  R  D  E  W  E  G  C  E  I  P  N  A
 O  T  E  I  S  F  M  S  S  H  G  E  T  E
 Y  E  O  E  N  T  H  P  E  L  N  H  B  A
```

Letters adjacent to E must occur within these limits.

From the limits of the letters adjacent to the letter E the letters W and L of ACKNOWLEDGE can only come from columns 6 and 2 respectively. These columns therefore may be added to the already juxtaposed columns 10 4 8:

```
        6 2 10 4 8
        ----------
        E   C R E
        S   S E M
        N Y E O H
        A D Q U A
        W Y O R K
        T S T W E
        R L O A D
        S P R O D
        S E D O U
        N E S E A
        Y C I T Y
(ACKNO) W L E D G (E)
        F T H I S
        T E L E P
```

It is obvious that these columns are correct and at this point solution is virtually assured. The student himself may complete solution.

It should be realized that in the elimination of key-lengths up to key-length 14, use was made of the almost invariable bigraph QU. Each of the eliminated key-lengths could just as well have been eliminated by using as the basic letter, not Q, but G (which occurred twice in the message)—and if the remaining letters of the probable word ACKNOWLEDGE could not be found within the limits obtained, the key-length could be rejected.

Another line of attack against this problem might also have been by using the idea of the invariable bigraph QU falling above or below the probable word ACKNOWLEDGE in the enciphering matrix. In our solution above we used this possibility after identifying a particular key-length and a particular QU bigraph. However, the problem might initially have been approached through this possibility without first having identified a particular key-length and a particular bigraph QU.

Thus, in the message text there is but one letter Q and three U's. It is evident that one of the U's will follow the single Q. We may therefore write down these possible combinations (QU) with extensions of text above and below the formed bigraph as follows:

Y I	Y S	Y S
M V	M N	M S
B O	B Y	B E
S C	S W	S M
C P	C F	C H
F T	F T	F A
P T	P R	P K
C R	C C	C E
S E	S L	S D
E O	E S	E D
100 QU 34	100 QU 71	100 QU 83
O R	O R	O A
T W	T S	T Y
O A	O S	O G
R O	R E	R S
D O	D M	D P
S E	S H	S R
I T	I A	I Y
E D	E K	E M
H I	H E	H B
L E	L D	L S

The numbers on both sides of the columns above are the respective positions of the letters Q and U in the cipher-text message. We now search the formed extensions for bigraphs formed by successive letters from the word ACKNOWLEDGE. Three such bigraphs are found:

```
        Y I                 Y S                 Y S
        M V                 M N                 M S
        B O                 B Y                 B E
        S C                 S W                 S M
        C P                 C F                 C H
        F T                 F T                 F A
        P T                 P R                 P K
        C R                 C C                 C E
        S E                 S L                 S D
        E O                 E S                 E D/
  100   Q U   34      100   Q U   71      100   Q U   83
        O R                 O R                 O A
        T W                 T S                 T Y
        O A                 O S                 O G
        R O                 R E                 R S
        D O                 D M                 D P
        S E                 S H                 S R
        I T                 I A                 I Y
        E D/                E K                 E M
        H I                 H E                 H B
        L E/                L D                 L S
```

Let us consider first the bigraph ED in the right-hand column above. If the bigraph ED comes from the word ACKNOWLEDGE, the ED must be followed by the letter G. In the cipher-text message the letter G occurs twice. Visually we can see also that immediately below the ED is the bigraph QU. Since QU is invariable followed by a vowel, we can note which letter G in the cipher-text message is followed by a vowel. In one case G is followed by the letter S and in the other case by the letter N. Therefore, since no vowel follows G in the message proper, we can consider that the bigraph ED in the right-hand column is in-valid and does not come from the word ACKNOWLEDGE. This leaves, therefore, only two bigraphs to consider, both in the first column on the left. Of these two bigraphs let's consider the bigraph ED. As before, the bigraph ED must be followed by the letter G; and since there are only two G's in the message, it is easy enough to juxtapose both G's against the left-hand column above:

Y I C	Y I T
M V L	M V O
B O S	B O R
S C U	S C D
C P R	C P S
F T S	F T I
P T S	P T E
C R E	C R H
S E M	S E L
E O H	E O I
Q U A	Q U E
O R K	O R R
T W E	T W R
O A D	O A Y
R O D	R O E
D O U	D O E
S E A	S E C
I T Y	I T I
(A C K N O W L)E D G(E)	(A C K N O W L)E D G(E)
H I S	H I N
L E P	L E P

Paying particular attention to the trigraphs between the QU- and EDG it is probable that the juxtaposition of columns on the right is incorrect. OAY for example is an almost impossible combination of plain-text letters, as is DOE and ROE, though the latter could possibly arise from ZERO EIGHT. On the other hand, the juxtaposition of columns on the left looks good up as far as QUA. EOH looks impossible, and it appears that if the juxtaposition of columns on the left is a correct juxtaposition of columns, the trigraph QUA is on the top line of the enciphering matrix. Assuming then that the juxtaposition on the left is correct, we note that the letter L occurs five times in the message. Let us juxtapose each of these five L's against the juxtaposition of columns on the left above as follows:

(1)	(2)	(3)	(4)	(5)
IQUA	DQUA	SQUA	TQUA	PQUA
EORK	YORK	NORK	OORK	EORK
OTWE	STWE	YTWE	RTWE	HTWE
OOAD	LOAD	WOAD	DOAD	NOAD
YROD	PROD	FROD	SROD	OROD
DDOU	EDOU	TDOU	IDOU	CDOU
YSEA	ESEA	RSEA	ESEA	ESEA
SITY	CITY	CITY	HITY	AITY
LEDG	LEDG	LEDG	LEDG	LEDG
PHIS	THIS	SHIS	IHIS	SHIS
ELEP	ELEP	ULEP	ELEP	NLEP

Examining the juxtapositions of columns above, particularly noting high-frequency or "good" combinations of letters, it is quickly seen that the juxtaposition (2) looks particularly good. Therefore, at this point let us analyze this juxtaposition (2) more closely. Particularly, let us determine the positions where the letters D Q U A occur within the cipher-text message:

Sequence of letters—	D	Q	U	A
Where letters occur—	12	100	34	78

If these four letters, DQUA, are adjacent in the enciphering matrix, *they will be separated in the final cipher-text message by a multiple of column lengths.*[1]

Therefore, let us examine the intervals between these letters:

Letter	Position	Interval
D	12	22
U	34	44
A	78	22
Q	100	

From the intervals between these letters it certainly appears as if a column length of 11 or 22 is involved. If we consider the column length to be 22, the letter D of DQUA, in position 12 will be in the middle of a column—since the first 22 letters of the cipher-text will be column 1. However, we have already determined that DQUA is probably on the top of the enciphering matrix. Therefore, the letter D of DQUA will not be in the middle of a column, but instead will be at the top of a column. In which case, with the D of DQUA being in position 12, a column length of 11 is perfect! We can therefore conclude that at least nine columns of length 11 are involved, since the interval between D in position 12 and Q in position 100 is 88 which must be a multiple of columns $(8 \times 11 = 88)$. The only key-length which gives rise to nine columns of 11 is key-length 14 which will produce eleven columns of length 11 and three of length 10, expressed in short form:

---

[1] See Chapter XII.

$$151 = \begin{matrix} 11-11\text{'s} \\ 3-10\text{'s} \end{matrix}$$

Thus, in short we have analytically determined the key-length 14 from the positions of letters in the cipher-text—these letters known to be adjacent in the enciphering matrix.

Problems

51. Probable word ENEMY.

IOREN NREIU TEARY NSTWL WCPEN
GANRF ATSLL ACHPD IREAA LKOOD
FTPGC AOONR OMIET TS

52. Probable word QUESTION.

ORMET LIIIA MHPIM EUTET IBEDD
SARNS RXEHT TOGEW AROQS SEDMB
EIEHF INEEH ANIEL ELNN

53. Probable word ALEXANDER.

POWRN EXRCO SSLSU FEDIF ABEAI
TEVES ONNTO ALTED ILB

54. Probable word SIX O'CLOCK.

TCTBT KYPTP USTOU PONEM NUXTO
EEHNW OCEKN EOIES OSIOO IIFLS
ELNCL FODEO LMOCI NTGPE ALACA
PF

55. Probable word WILLIAMS.

DTSOV HCTPS RVBCW SHTIY EIOLT
UAEEO NMWTT DTNTS AEIOE OIEAC
SCNNN NIORR EDAIL SOPTE CCIAP
STNIT TIEYO

56. Probable word OLYMPIC.

WOTYT RPTKA BWTCN RHORF MHLAA
OACLR EPRTE IHFOG OEGTE OYENT
TCEEC POTIO HISRL IRNME SBSSP
LOXII OTXA

57. Probable word MESSAGE.

LPEYS OWSNO ECLEE BMLLU TIAGB
CHINS EKOPI SLGR

58. Probable word KNOXVILLE.

EWKSO IIVID WEHED CUDDE NDEQE
ELENA OINPS EBBVP HNELL ANTWE
OEDOO DOBIF LXYCE ROEIE ITDWE
LEOGS RTDNL IAAES RNEHH LSIND
NPVOL OAEME NULRC HP

59. Probable word INFORMATION.

EHAIP VIYCD AOONC LUNEK SMTLT
GOMFO AWETN ANCUO LSDMO TOIOE
POEIY SCSYR RISSE RBFEE ROSET
PUINB FARND XTTOR DAREE OYTEN
SRAUT IDTAA RNINT NPPLA TOOEN
OAVRR NIMIS IHTUE

60. Probable word SOUTH.

FIWDK MFIZT VNSUS TARNE EHOPA
GEEHS CTEWE NEAPW LILLT RISBE
RLOOF EILOE LRFOR RLNHA AIOAS
CEESW TTON

Chapter XIV

Cryptanalytic Solution

Given: The Key-Length

In this chapter we approach the edge of the general solution of the single columnar transposition cipher. In this chapter we are given as our only assist towards solution, the key-length. Since there are but a limited number of possible key-lengths, one general solution might be the successive testing of various possible key-lengths. The length of time it takes to test a particular key-length is indeed the crux of this chapter. This length of time depends upon the particular cipher-text message or cryptogram. In fact, it is impossible to state for all cases how long it will take to test a particular key-length. The only completely reliable test is to actually solve the cipher—which indeed thereby proves the key-length—though a key-length may be tested in a manner similar to that shown in Chapter XI. In this respect, however, while Chapter XI concerned itself only with the "completely filled matrix," this somewhat similar test made of the "incompletely filled matrix" offers unfortunately a much less degree of reliability. In the latter part of this chapter this particular test will be taken up.

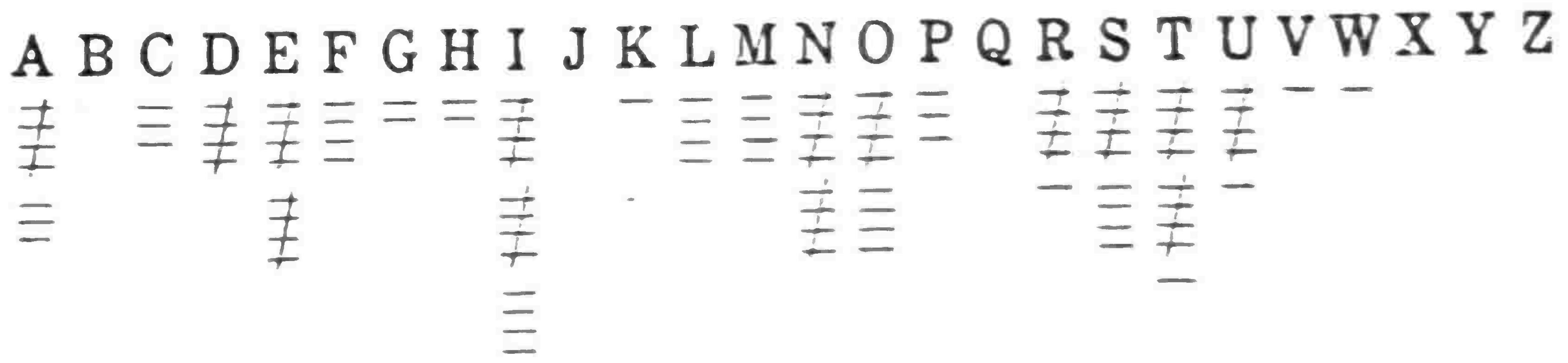
Given the key-length of the cipher-text message, solution will depend upon various factors. Amongst these factors are: the length of the message, the length of the key, the particular plain-text being enciphered, and even such a thing as the "good fortune" of the cryptanalyst. Let us go through the process of solution. We are given the following cryptogram with the known key-length 12:

```
OFFTE  ASMTN  RAPSM  COIWA  RNSOI
DPSOA  ESCPG  TRFHH  TTDNI  SOTII
DFNIO  TNTSA  DLUEU  IMRUI  EKAME
NLDIT  LTANI  EIEIO  LSENC  OOSRU
UINUI  VTEAG  NRE
```

Since we are given the key-length 12, we can easily construct the analytic matrix:

1	2	3	4	5	6	7	8	9	10	11	12
				R	S	O	E				
			S	F	O	T	U	M			
		W	O	H	T	N	I	E	N		
	N	A	A	H	I	T	M	N	I	N	
O	R	R	E	T	I	S	R	L	E	C	U
F	A	N	S	T	D	A	U	D	I	O	I
F	P	S	C	D	F	D	I	I	E	O	V
T	S	O	P	N	N	L	E	T	I	S	T
E	M	I	G	I	I	U	K	L	O	R	E
A	C	D	T	S	O	E	A	T	L	U	A
S	O	P	R	O	T	U	M	A	S	U	G
M	I	S	F	T	N	I	E	N	E	I	N
T	W	O	H	I	T	M	N	I	N	N	R
N	A	A	H	I	S	R	L	E	C	U	E

We can also easily tabulate the monoliteral frequency distribution of the message:



At this point let's take a look at Figure 5 on the next page which is a listing of the one hundred most frequent trigraphs in the English language.

It will be noted that the letter G occurs in only one of the 100 most frequent trigraphs, ING, which is one of the ten most frequent trigraphs. From the monoliteral frequency distribution we see that the letter G has occurred twice. Is it unreasonable to assume that one of these G's might have occurred in or from the trigraph ING? Let us test this assumption. In the analytic matrix let us circle one of the G's. At the same time let us find the "limits" of adjacent letters to the letter G. We thus have the following:

THE 100 MOST FREQUENT TRIGRAPHS

AIN*
ALL*
AME
AND**
ANT
ANY
ARD
ARE*
ART
AST
ATE**
ATI*
AVE

BUT

COM
CON*
DAY
DER
DES
DIN

EAR
ECT
EEN
ENC
ENT**
ERA
ERE**
ERS*
ESS
EST*
EVE*

FOR**
HAS
HAT*
HER**
HIS*
HOU

ICA
ICH
ILL*
INE
ING**
INT
ION**
ITH*
IVE

LAR
LES
LIN

MAN*
MEN

NCE*
NDE
NOT
NTE

OME
ONE
ONS
ORE
ORT
OUN
OUR
OUS
OUT
OVE

PER
PRE
PRO

RAT
REA
RED*
RES*
ROM

SAN
STA
STE
STI
STR
TED*
TER*
TES
THA*
THE***
THI
THO
TIC
TIN
TIO**
TRA
TUR

UND
URE

VEN
VER*
WAS
WER
WHE
WHI
WIL
WIT

*** most frequent trigraph.
** ten most frequent trigraphs.
* next most frequent 20 trigraphs.

FIGURE 5.

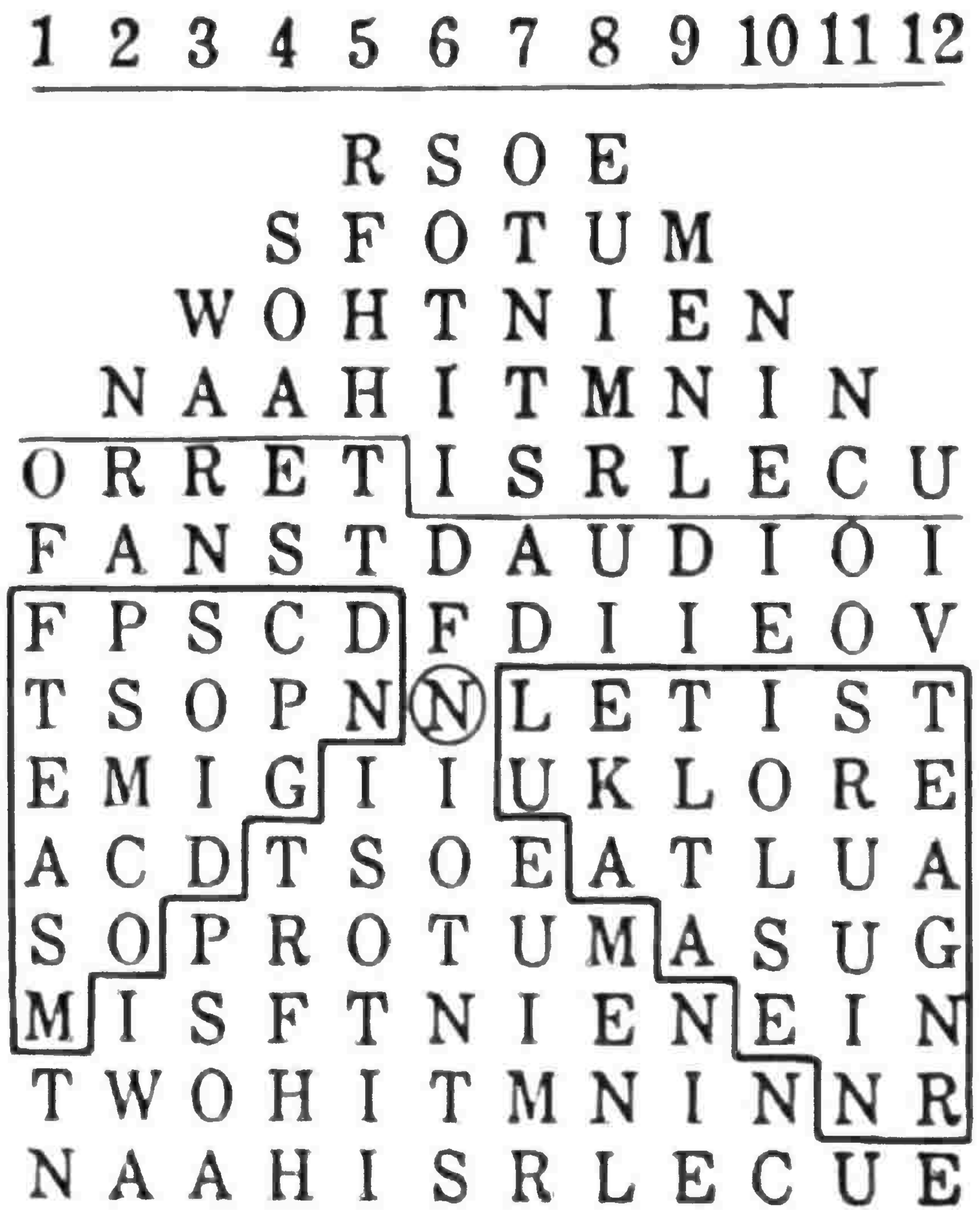
1	2	3	4	5	6	7	8	9	10	11	12
				R	S	O	E				
			S	F	O	T	U	M			
		W	O	H	T	N	I	E	N		
	N	A	A	H	I	T	M	N	I	N	
O	R	R	E	T	I	S	R	L	E	C	U
F	A	N	S	T	D	A	U	D	I	O	I
F	P	S	C	D	F	D	I	I	E	O	V
T	S	O	P	N	N	L	E	T	I	S	T
E	M	I	G	I	I	U	K	L	O	R	E
A	C	D	T	S	O	E	A	T	L	U	A
S	O	P	R	O	T	U	M	A	S	U	Ⓖ
M	I	S	F	T	N	I	E	N	E	I	N
T	W	O	H	I	T	M	N	I	N	N	R
N	A	A	H	I	S	R	L	E	C	U	E

It is noted upon examination of the "limits" of adjacent letters that there are only two possible letter N's which might be adjacent to the letter G—one of these is in column 5 and the other is in column 6. Let's put each of these N's next to the letter G and see how the juxtaposed columns look. Even better, we can use the *letter contact weight chart* (Figure 3) shown on page 55 and obtain a validity weight for each of the juxtapositions.

5	12	1
R		
F	U	1
H	I	2
H	V	0
T	T	2
T	E	2
D	A	2
N	G	2
I	N	3
S	R	0
O	E	0
T		
I		14
I		

6	12	
S		
O	U	3
T	I	3
I	V	2
I	T	2
D	E	2
F	A	1
N	G	2
I	N	3
O	R	2
T	E	2
N		
T		22
S		

The juxtaposition of columns 6 and 12, yielding a validity weight of 22, looks excellent at this point. Using the letter N in column 6 as the "basic letter", let us obtain the "limits" of adjacent letters—as was done with the letter G as the "basic letter."

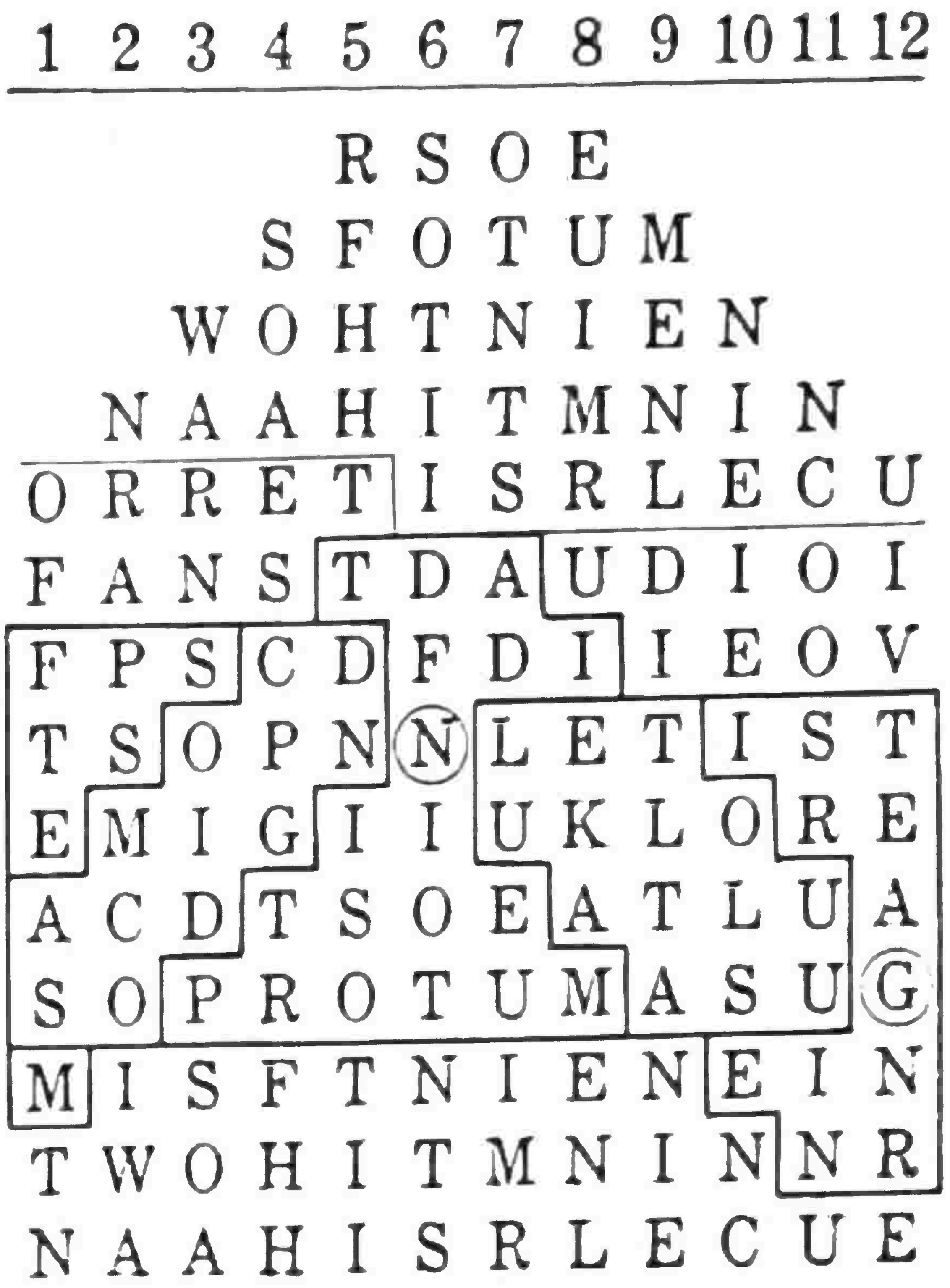


```
 1  2  3  4  5  6  7  8  9 10 11 12
             R  S  O  E
          S  F  O  T  U  M
       W  O  H  T  N  I  E  N
    N  A  A  H  I  T  M  N  I  N
 O  R  R  E  T  I  S  R  L  E  C  U
 F  A  N  S  T  D  A  U  D  I  O  I
 F  P  S  C  D  F  D  I  I  E  O  V
 T  S  O  P  N  N  L  E  T  I  S  T
 E  M  I  G  I  I  U  K  L  O  R  E
 A  C  D  T  S  O  E  A  T  L  U  A
 S  O  P  R  O  T  U  M  A  S  U  G
 M  I  S  F  T  N  I  E  N  E  I  N
 T  W  O  H  I  T  M  N  I  N  N  R
 N  A  A  H  I  S  R  L  E  C  U  E
```

If the letter N in column 6 and the letter G in column 12 are adjacent in the enciphering matrix (as we presume them to be, since their columns yield a validity weight of 22), the limits of adjacent letters as obtained will be valid for both the basic letter G and the basic letter N. Since the term *adjacent letters* refers to letters adjacent within a key-length[1], we can combine the limits of adjacent letters as found for the basic letter N and as found for the basic letter G. Thus the more narrow limits of adjacent letters to the pair of letters NG is the following:

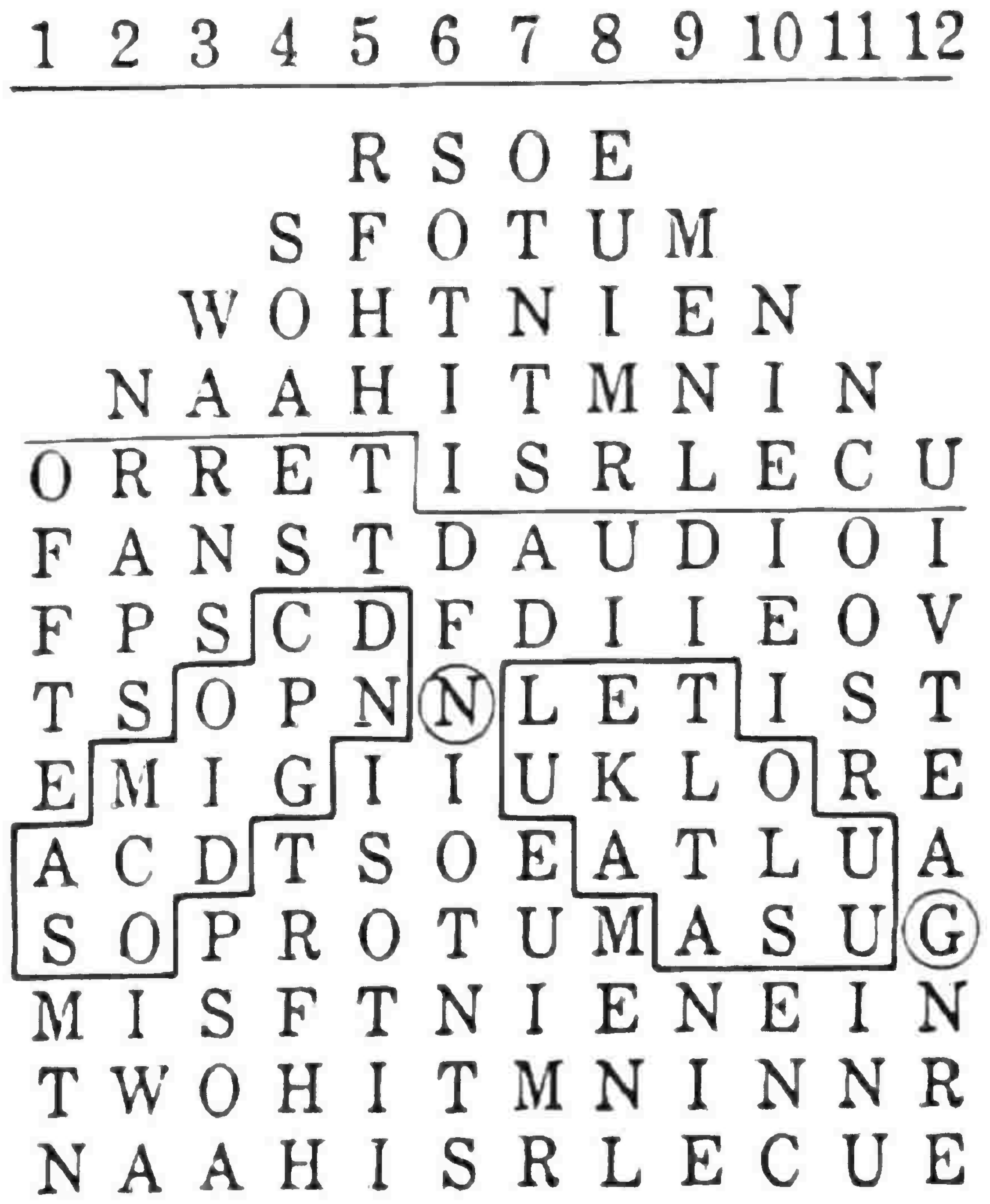
---

[1] See pages 86-88 for discussion of "adjacent letters".



```
  1  2  3  4  5  6  7  8  9 10 11 12
              R  S  O  E
           S  F  O  T  U  M
        W  O  H  T  N  I  E  N
     N  A  A  H  I  T  M  N  I  N
  O  R  R  E  T  I  S  R  L  E  C  U
  F  A  N  S  T  D  A  U  D  I  O  I
  F  P  S  C  D  F  D  I  I  E  O  V
  T  S  O  P  N  Ⓝ  L  E  T  I  S  T
  E  M  I  G  I  I  U  K  L  O  R  E
  A  C  D  T  S  O  E  A  T  L  U  A
  S  O  P  R  O  T  U  M  A  S  U  Ⓖ
  M  I  S  F  T  N  I  E  N  E  I  N
  T  W  O  H  I  T  M  N  I  N  N  R
  N  A  A  H  I  S  R  L  E  C  U  E
```

which results in:



```
  1  2  3  4  5  6  7  8  9 10 11 12
              R  S  O  E
           S  F  O  T  U  M
        W  O  H  T  N  I  E  N
     N  A  A  H  I  T  M  N  I  N
  O  R  R  E  T  I  S  R  L  E  C  U
  F  A  N  S  T  D  A  U  D  I  O  I
  F  P  S  C  D  F  D  I  I  E  O  V
  T  S  O  P  N  Ⓝ  L  E  T  I  S  T
  E  M  I  G  I  I  U  K  L  O  R  E
  A  C  D  T  S  O  E  A  T  L  U  A
  S  O  P  R  O  T  U  M  A  S  U  Ⓖ
  M  I  S  F  T  N  I  E  N  E  I  N
  T  W  O  H  I  T  M  N  I  N  N  R
  N  A  A  H  I  S  R  L  E  C  U  E
```

If we continue with our original assumption that the letter G in column 12 has occurred in the trigraph ING, it will be seen from the above limits of adjacent letters that there is but one letter I which can preceed the bigraph NG (from columns 6 and 12). This is the letter I in column 3. Therefore, let us juxtapose column 3 in front of columns 6 and 12.

3	6	12
	S	
W	O	U
A	T	I
R	I	V
N	I	T
S	D	E
O	F	A
I	N	G
D	I	N
P	O	R
S	T	E
O	N	
A	T	
	S	

The three juxtaposed columns look excellent and it appears that at this point we have a good "foot in the door" towards solution. At this point the student with three matched columns plus the limits of adjacent letters above (still valid for letters adjacent to ING) should have no trouble in completing solution.

For now let us leave matched columns and return to the beginning of this chapter where the identification of key-length was discussed. It was stated that the only true completely reliable test of a key-length was the actual reading of the message, i.e., solution. However, mention was made that there is another test, similar to the test in Chapter XI which might give an indication as to the validity or non-validity of a particular key-length without the actually reading of the message itself. Let's examine this test which admittedly lacks the degree of reliability that the test of Chapter XI had with respect to the "completely filled matrix" key-length.

The theory of this test, similar to the theory of the test in Chapter XI, is based upon the fact that vowels will be evently distributed throughout a plain-text message.

Consider the cipher-text message of this chapter. Since we know the key-length to be 12, let us first test this key-length.

We turn to the analytic matrix (for key-length 12) and disregarding most of the cap, we circle and count the number of vowels in each row as follows:

												Vowels
Ⓞ	R	R	Ⓔ	T	Ⓘ	S	R	L	Ⓔ	C	Ⓤ	5
F	Ⓐ	N	S	T	D	Ⓐ	Ⓤ	D	Ⓘ	Ⓞ	Ⓘ	6
F	P	S	C	D	F	D	Ⓘ	Ⓘ	Ⓔ	Ⓞ	V	4
T	S	Ⓞ	P	N	N	L	Ⓔ	T	Ⓘ	S	T	3
Ⓔ	M	Ⓘ	G	Ⓘ	Ⓘ	Ⓤ	K	L	Ⓞ	R	Ⓔ	7
Ⓐ	C	D	T	S	Ⓞ	Ⓔ	Ⓐ	T	L	Ⓤ	Ⓐ	6
S	Ⓞ	P	R	Ⓞ	T	Ⓤ	M	Ⓐ	S	Ⓤ	G	5
M	Ⓘ	S	F	T	N	Ⓘ	Ⓔ	N	Ⓔ	Ⓘ	N	5
T	W	Ⓞ	H	Ⓘ	T	M	N	Ⓘ	N	N	R	3
N	Ⓐ	Ⓐ	H	Ⓘ	S	R	L	Ⓔ	C	Ⓤ	Ⓔ	6

We realize that the vowels on one row of the analytic matrix will not be on the same row in the enciphering matrix—as was the case in Chapter XI—however we can say generally speaking that the vowels in the upper half of the analytic matrix will be in the upper half of the enciphering matrix. Thus, in a valid analytic matrix the number of vowels in the upper half of the matrix (less cap) will approximate the number of vowels in the lower half. Let us count the number of vowels in the two "halves" above:

Vowels	*Totals*
5	25
6	
4	
3	
7	
6	25
5	
5	
3	
6	

Since the two halves each have the same number of vowels, we can say that the vowel distribution of the analytic matrix is favorable towards "a valid analytic matrix." Let us now test a key-length which we know to be in-valid, i.e., a key-length of 14:

														Vowels
Ⓞ	T	Ⓞ	Ⓘ	C	T	Ⓘ	N	Ⓤ	Ⓐ	L	Ⓘ	Ⓞ	Ⓘ	9
F	N	Ⓘ	D	P	T	Ⓘ	T	Ⓘ	M	T	Ⓞ	S	V	4
F	R	W	P	G	D	D	S	M	Ⓔ	Ⓐ	L	R	T	2
T	Ⓐ	Ⓐ	S	T	N	F	Ⓐ	R	N	N	S	Ⓤ	Ⓔ	5
Ⓔ	P	R	Ⓞ	R	Ⓘ	N	D	Ⓤ	L	Ⓘ	Ⓔ	Ⓤ	Ⓐ	8
Ⓐ	S	N	Ⓐ	F	S	Ⓘ	L	Ⓘ	D	Ⓔ	N	Ⓘ	G	6
S	M	S	Ⓔ	H	Ⓞ	Ⓞ	Ⓤ	Ⓔ	Ⓘ	Ⓘ	C	N	N	7
M	C	Ⓞ	S	H	T	T	Ⓔ	K	T	Ⓔ	Ⓞ	Ⓤ	R	5
T	Ⓞ	Ⓘ	C	T	Ⓘ	N	Ⓤ	Ⓐ	L	Ⓘ	Ⓞ	Ⓘ	Ⓔ	9

Since there are an odd number (9) of rows, in order to count the two "halves," we shall disregard the middle row:

Vowels	*Totals*
9	20
4	
2	
5	
8	
6	27
7	
5	
9	

It is noted that the upper half of the analytic matrix contains seven less vowels than the lower half. We can say then that this distribution of vowels is not favorable towards "a valid analytic matrix."

To finalize this chapter it should be stated that "column matching" is more of an art rather than a science and that with practice one can become very adept at juxtaposing columns almost visually. The idea of limiting adjacent letters as was done in this chapter is somewhat theoretical and was introduced to give the student background; for a good cryptanalyst could certainly have easily solved the message without the somewhat tedious analytic steps which we went through. However, the student having learned the principle has a tool when he needs it!

Problems

61. Key-length 14.

CEUSE TNAIY NNFHE ALHFA ILFNF
MUCSU NOOOT MHCTR CODRS OPMOO
ESPDN ITNAT ELEPQ IERIT FCDLE
AEIOE IQOIP YNETN IOOEN ESXAT
CCAAI HRRYY SHEIR EEMRO ANFNT
UCORT IWFLR WTTEL TOTRT

62. Key-length 11.

EVGOX TAEUU NBTBF SSSUR NWEER
FRMHR CPIAT ISIBF RELDF TETDD
EOLEA KRTPL ISOLN SSEDL LTIRR
EIEOE TTVEO OOTTW NISED MOUAO
ITNLE OAVEN LHI

63. Key-length 8.

ENMRE NLUCO YIVII ORETE NYIEC
ANACV OVVOT EREIF EENOO EDILR
TFRRI TFSNI MFICH FN

64. Key-length 10.

REAUO AUGOO ILTHH OTTDT SIEEA
OPHEN ENTTS BCLEN TMWEN EKEFT
UOSBU TTPTH IHOSR YTCSP HDJOH
DOLEM IRTVL NGGTU RNENI OIISP
OACH

65. Key-length 10.

RFAAT SACCT ATRAU LUTOE APCMT
AWDAN HRTTS DGONS TIHOE PHNTE
TRNIC ORNPP VMUML AHHIO EIINO
NHUOG CREET OOSST HTRTT ERRSS
SSSTA T

66. Key-length 9.

ILSTA ATRIE OEEPR ECCIA ELGSN
TGVRB EDAET AOEOT EDEPN SRTAP
OLLRN XRCNY HPNNR OTUFL OFLLF
NROIR NURCA OIERT SEWC

67. Key-length 8.

KDTNP ETTIT EDEHI OLPEI OPESA
EKSAF AATCR EANSI ODNAM TMEWS
OTSLN CSSCE OOONN TPMT

68. Key-length 7.

OIUTC RTREH FCMIB SENTW IAEOL
OGPRC DOONS KDROR HNSLE KO

69. Key-length 6.

AXISR EDOSG ASCOA SODYN MEUNC
NASRB TEFN

70. Key-length 10.

REEHS PSAFT REPNL NPITO YUDNS
OESSR EGPYS WTBSA REFET SAIIE
TDIYA WOYAS AOLET FHNFI ENVAI
OCNUM IGSTD ETNIN STPTL EOVCS
NTPOR SSLED TIIS

Chapter XV

Cryptanalytic Solution

The General Solution

In previous chapters we have considered the solution of the single columnar transposition cipher given various types of "assists", such as knowing a probable word, being given the key-length, etc. These "assists" by no means are improbable situations. With but a limited number of key-lengths, for example, the cryptanalyst may simply try one key-length after another until solution is reached. The same holds true of probable words. The cryptanalyst may guess or reason that a particular probable word is in a message, test the guess, and if results are negative, he may simply try another probable word. The cryptanalyst's procedure in a manner of speaking may be compared to that of the flow of electricity. Electricity flows along the path of least resistance. Similarly, the cryptanalyst's normal procedure is to arrive at a cryptanalytic solution with the least amount of work, trouble, testing, etc. This path of least resistance in the cryptanalyst's solving of a single columnar transposition cipher might be a "trial-and-error" technique such as we previously have considered. More likely, however, it will be a "general solution" technique. This chapter takes up this "general solution" technique.

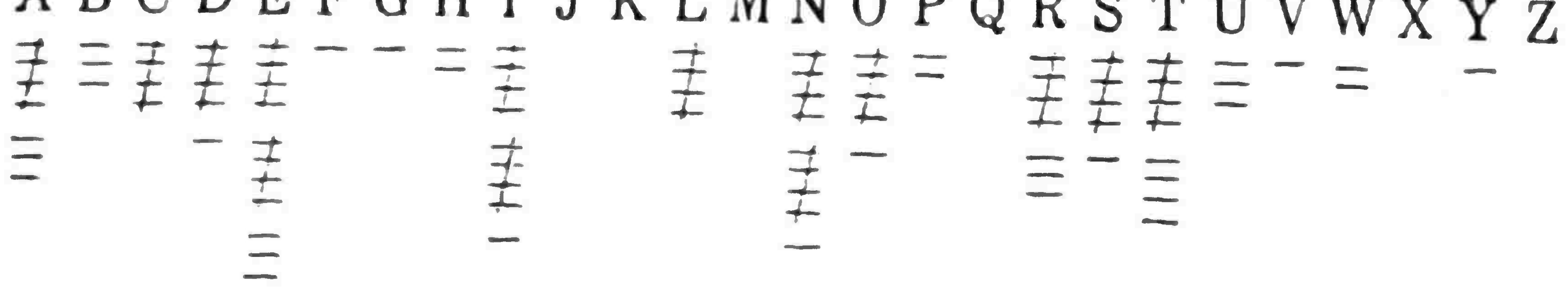
Consider the following cipher-text message:

NCAAO TUAOG SVLIW HAIOH EENIR
DRBNR UEART IRCNO NENNA LWSSD
OSNEP TLAPR TTEER BTEAT INDIR
TDCIS EENIE TONEB DSLDE IUYCI
CFLI

Let us first determine the possible column lengths for this pa ticular message. The key-length used to encipher this message most probably lies between 6 and 15. Therefore, let us compute the column lengths for these possible key-lengths.

Key-length	Column Lengths
6	2—18's 4—17's
7	6—15's 1—14
8	8—13's
9	5—12's 4—11's
10	4—11's 6—10's
11	5—10's 6— 9's
12	8— 9's 4— 8's
13	13— 8's
14	6— 8's 8— 7's
15	14— 7's 1— 6

The tabulation of a monoliteral frequency distribution is easily made:



We begin our analysis proper by attempting to "match" or juxtapose low-frequency letters. The ideal situation of course is when the letter Q occurs in the message. In the present instance since there is no letter Q in the message we will have to work with other low-frequency letters. For example, the letter L occurs in this particular message five times. Is it possible that in the enciphering matrix two of these L's have fallen together, i.e., that the bigraph LL occurs in the plain-text message. Let's examine this possibility.

Segments of cipher-text containing the letter L are taken out of the cipher-text message and put in vertical columns side-by-side. At the top of each column is put the position in the cipher-text message that the letter L in that column has occurred. We thus have the following:

13	46	57	93	103
A	N	S	N	Y
O	E	N	E	C
G	N	E	B	I
S	N	P	D	C
V	A	T	S	F
Ⓛ	Ⓛ	Ⓛ	Ⓛ	Ⓛ
I	W	A	D	I
W	S	P	E	
H	S	R	I	
A	D	T	U	
I	O	T	Y	

The first column with the letter L in position 13 also contains the letter V. Since the letter V is restricted in contact almost entirely to vowels, this first column can only be juxtaposed with another column such that the V will contact a vowel. The only possible column is the column with the letter L in position 46. Therefore, if the L in position 13 is envolved in the bigraph LL, the only possible juxtaposition of columns (such that V contacts a vowel) is the following:

13	46		46	13
A	N		N	A
O	E		E	O
G	N		N	G
S	N		N	S
V	A		A	V
L	L	or	L	L
I	W		W	I
W	S		S	W
H	S		S	H
A	D		D	A
I	O		O	I

The juxtaposition on the right looks particularly good. For example, the bigraph NG is excellent. For the moment than let's consider this juxtaposition further.

If this juxtaposition is correct, what key-lengths can give rise to this juxtaposition? The difference or *distance* between the L in position 13 and the L in position 46 is 33. Provided of course that the juxtaposition be correct, the 33 then will be a multiple of column lengths of the enciphering matrix. Consider the key-length 6 where the column lengths are $\frac{2\text{–}18\text{'s}}{4\text{–}17\text{'s}}$. The column lengths 17 and 18 will not fit into 33. Therefore, a key-length of 6 will not allow the juxtaposition of the L in position 13 with the L in 46.

The mathematical procedure for determining whether particular column lengths will fit into a given distance is as follows: *The short column length is divided into the distance. If the remainder is greater than the quotient, the columns will not fit into the distance. If the remainder is equal to or less than the quotient, the columns will fit into the distance.* Thus, in the case just considered the column lengths were 17 and 18, and the distance was 33. The short column length (17) is divided into the distance (33). The quotient is 1 and the remainder is 16. Since in this case the remainder is greater than the quotient, the lengths will not fit.

In a similar manner we can determine that the only key-lengths which will allow the above juxtaposition of L's (in position 13 and 46) are the following:

Key-Lengths	Column Lengths	Combination of Columns Giving Rise to Distance 33
9	5—12's 4—11's	3—11's
10	4—11's 6—10's	3—11's
12	8— 9's 4— 8's	1— 9 3— 8's

At this point let us return to our juxtaposition.

46	13
N	A
E	O
N	G
N	S
A	V
L	L
W	I
S	W
S	H
D	A
O	I

In front of the bigraph NG there will likely be the letter I, yielding the common trigraph ING. Immediately below the NG is the bigraph NS. In front of the NS will certainly be a vowel; and in front of the LL will also be a vowel. Let's examine the cipher-text message then for a segment as follows:

—
—
I
(vowel)
—
(vowel)
—
—
—
—
—

Only two possible segments are found and these juxtaposed against our already existing juxtaposition look as follows:

21	46	13
H	N	A
A	E	O
I	N	G
O	N	S
H	A	V
E	L	L
E	W	I
N	S	W
I	S	H
R	D	A
D	O	I

87	46	13
E	N	A
N	E	O
I	N	G
E	N	S
T	A	V
O	L	L
N	W	I
E	S	W
B	S	H
D	D	A
S	O	I

Note that the three column juxtaposition on the above left can only arise if the key-length is 12. For 21−13=8 and 8 cannot be a multiple of column lengths 10, 11, or 12 which are the column lengths found in the key-lengths 9 and 10. Instead, 8 can only be a multiple of a column length 8 found in key-length 12.

For the moment leaving the three column juxtaposition on the above left, let's examine the three column juxtaposition on the right above. The key-lengths 9 and 10 can be dispensed with almost immediately. Note the letters G and L in positions 10 and 13 respectively in the column on the right. If the column length is 10, 11, or 12 (for key-lengths 9 and 10), the letter G will be at the bottom or close to the bottom of a column and the letter L in position 13 will be in another column! In other words, if the key-length is 9 or 10, the letters L and G cannot be in the same column! Having dispensed with key-lengths 9 and 10, can these three juxtaposed columns arise from a key-length of 12? The distance between the L in position 46 and L in position 13 is 33 which is valid for key-length 12 since $\frac{1\text{–}9}{3\text{–}8\text{'s}}$ equals 33. Also the distance between the 0 in position 87 and L in position 46 is 41. Can this distance come from key-length 12? The answer is yes, for $\frac{1\text{–}9}{4\text{–}8\text{'s}}$ equals 41. But what is wrong?

If you remember, in the entire message with key-length 12 there are $\frac{8\text{–}9\text{'s}}{4\text{–}8\text{'s}}$. In the distance 33, 3−8's have been used, and in the distance 41, 4−8's have been used. This is a total of 7−8's! This is impossible since there are only 4−8's in the entire message (for key-length 12). In other words, the three column juxtaposition on the above right cannot have occurred from a key-length of 12. Therefore, we need only consider the three column juxtaposition on the above left as being possible; and moreover, we have already found that the juxtaposition can arise only if the key-length is 12!

Let us construct then the analytic matrix for key-length 12 together with the limits of adjacent letters for the L in position 13 and the L in position 46:

1	2	3	4	5	6	7	8	9	10	11	12
				A	E	O	R				
			R	R	N	S	T	A			
		A	D	T	N	N	T	T	C		
	O	I	R	I	A	E	E	I	I	O	
N	G	O	B	R	L	P	E	N	S	N	I
C	S	H	N	C	W	T	R	D	E	E	U
A	V	E	R	N	S	L	B	I	E	B	Y
A	Ⓛ	E	U	O	S	A	T	R	N	D	C
O	I	N	E	N	D	P	E	T	I	S	I
T	W	I	A	E	O	R	A	D	E	L	C
U	H	R	R	N	S	T	T	C	T	D	F
A	A	D	T	N	N	T	I	I	O	E	L
O	I	R	I	A	E	E	N	S	N	I	I

1	2	3	4	5	6	7	8	9	10	11	12
				A	E	O	R				
			R	R	N	S	T	A			
		A	D	T	N	N	T	T	C		
	O	I	R	I	A	E	E	I	I	O	
N	G	O	B	R	Ⓛ	P	E	N	S	N	I
C	S	H	N	C	W	T	R	D	E	E	U
A	V	E	R	N	S	L	B	I	E	B	Y
A	L	E	U	O	S	A	T	R	N	D	C
O	I	N	E	N	D	P	E	T	I	S	I
T	W	I	A	E	O	R	A	D	E	L	C
U	H	R	R	N	S	T	T	C	T	D	F
A	A	D	T	N	N	T	I	I	O	E	L
O	I	R	I	A	E	E	N	S	N	I	I

Those limits that are common to both the above are the limits of adjacent letters for the bigraph LL, i.e.:

1	2	3	4	5	6	7	8.	9	10	11	12
				A	E	O	R				
			R	R	N	S	T	A			
		A	D	T	N	N	T	T	C		
	O	I	R	I	A	E	E	I	I	O	
N	G	O	B	R	Ⓛ	P	E	N	S	N	I
C	S	H	N	C	W	T	R	D	E	E	U
A	V	E	R	N	S	L	B	I	E	B	Y
A	Ⓛ	E	U	O	S	A	T	R	N	D	C
O	I	N	E	N	D	P	E	T	I	S	I
T	W	I	A	E	O	R	A	D	E	L	C
U	H	R	R	N	S	T	T	C	T	D	F
A	A	D	T	N	N	T	I	I	O	E	L
O	I	R	I	A	E	E	N	S	N	I	I

And the three column juxtaposition containing the trigraph ING is the juxtaposition of columns 3, 6, and 2 respectively.

3	6	2
A	E	O
I	N	G
O	N	S
H	A	V
E	L	L
E	W	I
N	S	W
I	S	H
R	D	A
D	O	I
R	S	
	N	
	E	

Using the symbol (c) for *consonant* and (v) for *vowel* let's see which categories of letters will preceed the trigraphs formed by the three column juxtaposition above.

	3	6	2
—	A	E	O
(c)	I	N	G
—	O	N	S
—	H	A	V
(c)	E	L	L
(c)	E	W	I
(v)	N	S	W
(c)	I	S	H
(v)	R	D	A
—	D	O	I
	R	S	
		N	
		E	

Our object now is to find this particular column among the remaining unidentified nine columns of the analytic matrix. The consonant which preceeds the trigraph ELL will of course fall within the limits of adjacent letters found on page 123; and if such a column exists is should easily be found. Column 5 fits perfectly:

```
         5
        ---
         A
   —     R
  (c)    T
   —     I
   —     R
  (c)    C
 -----------
  (c)    N
  (v)    O
  (c)    N
  (v)    E
   —     N
         N
         A
```

Column 5 therefore may be juxtaposed against the first three columns:

```
5 3 6 2
-------
A
R A E O
T I N G
I O N S
R H A V
C E L L
-------
N E W I
O N S W
N I S H
E R D A
N D O I
N R S
A   N
    E
```

The four letters IONS strongly suggest that the letter T precedes them. In the analytic matrix there is but one column containing the letter T which might fit, i.e., column 9. Therefore, column 9 may be added to the juxtaposition:

9	5	3	6	2
	A			
	R	A	E	O
A	T	I	N	G
T	I	O	N	S
I	R	H	A	V
N	C	E	L	L
D	N	E	W	I
I	O	N	S	W
R	N	I	S	H
T	E	R	D	A
D	N	D	O	I
C	N	R	S	
I	A		N	
S			E	

Column 9 looks excellent and there is little doubt but that we are on the right track! With the narrow limitations of the remaining columns solution is almost complete. It is left to the student to complete solution.

To summarize this general solution:

(1) Two segments of cipher-text are matched—usually through the finding of low-frequency "good" bigraphic letter combinations such as QU, LL, LY, NG, etc.

(2) This matching of segments allows the cryptanalyst to obtain a *distance* which being a multiple of column lengths limits the number of key-lengths that might give rise to the obtained distance.

(3) A third juxtaposed segment or two other matched segments will practically always define the key-length of the enciphering matrix.

(4) Given the key-length plus a "narrow" limit of adjacent letters, success is generally assured!

(5) Finally, of course, if all fails, the cryptanalyst may turn to

the "trial-and-error" method of simply trying a limited number of key-lengths, using procedures set forth in Chapter XIV, or the probable word method following the method of Chapter XIII.

Problems

71. EOETP BCGOC IAARC RREAF IOTEF
LRNAT MEOIE UHJOA TLIEW DMNDF
RANUO NHYNL ISSOI UOUIN NHIRL
ITRNR VNRBC TF

72. TCEUT RWNCP MEHKE IOARR FHHSI
AEESO ITRNU TSCEO QSEAD DIGLN
OEETM DSEHV EPNOB TYNVQ SOSGA
PEBER IOESF IIIUP TTE

73. GLVOO ITTCN SNIID TNOET BUMET
IEINO RPEEE METII ZFTSF AOEHE
SEHES VNGHL ORBXH SKILW ETGNO
HLVED NNOHT CEUEO TLNON H

74. NVSNA BSUCN ORNET AUCSO EONHI
SENEN WPOCE LOPOE EINOT MRTST
MSEFE MEPRF NRLRE DEHQI YTBAI
TURSE TEPCN ISTNE TROEO MNNCF
EEITE IAMAT SEPTS LCELH RAENE
AATRB POOEW BWUGO LFNOS DSENR
UTEMR USPRE FOOTS ALERV EIDEO
DLTPP T

75. PTTOL ILTEF SGTAT OEDPF RSNVN
PEANC RUINH GLHHN EFIOA EOBIT
NPAIA AHTO

76. OHCMF SIOLS TISGA LIHNS EFANS
OTWDT AFTGI NHOVA ROHIL CGEAL
OSTLR LNNSD HIGEI UGAWC ISOST
RRIRT EUPTN UEE

77. OTOOS ERRIS FIMRE VTSDT TCCCL
WOECE RUNEA OPPCD RENTS TRNEN
OORIR FHPAA YDESO AIOSG RTYPT
FXSPU PELED OEDSE IWER

78. EABDE OPRIN PSEYH GEVUI TCDET
TOETR ELVTY TDNEH HCOIH PERCL
LEBNN KCLOO OEURT URTEN UIATS
NUHEL RYTIE OFT

79. KPNEI GDYTI TLATO LTHRI EWDRA
FEEEU PMOSC SOCYN LASTN YANIR
AIEDN EOAFR AAMOA TAGUT TSDEB
TODNR OOHDN TSSEN H

80. OEHSO GPMEU MIABS ONRLD LOGLA
TWEIL ARTKW EURH

Chapter XVI

Final Remarks

I think that it will be agreed that in previous chapters we have covered the single columnar transposition cipher quite completely. In fact, I am sure that by this time the student must realize that the single columnar transposition cipher presents really but little actual cryptanalytic difficulty. Determining factors in solution are various factors within the text of the message itself (does the text contain the letter Q, etc.) and even these factors do not actually determine whether or not the message can be read, but rather, how long it will take to read the message!

In this chapter we shall mention several "odds and ends" that have been missed or perhaps have lacked emphasis in previous chapters. In a sense then this chapter might be compared to the final "bow-knot" tied to what the author hopes to be a neat, well-tied package.

In previous discussions of key-lengths and message lengths, no mention was made of the fact that often correspondents will deliberately put *nulls*, letters having no significance, into the final portion of the plain-text message in order that the length of the cipher-text message will be a multiple of five, i.e., that all groups of the cipher-text will contain five letters.

Occasionally, correspondents will avoid the use of certain key-lengths, such as avoiding key-lengths of 5, 10, 15, 20, etc. This is sometimes done under the mistaken belief that this somehow prevents the formation of completely filled enciphering matrices.

How do these efforts of the correspondents affect cryptanalysis? If the key-length is restricted to "not multiples of five", the cryptanalyst obviously can narrow down key-length possibilities; and if the plain-text message has nulls added to the end of the text in order to make the message length a multiple of five, the addition of nulls might make solution easier. For example, nulls added to the end of the plain-text message might be the letters XXXX. If the cryptanalyst in his analysis notes an abnormal number of low-frequency letters (such as a number of X's), these low frequency letters might be nulls added to the end of the message.[1]

Considering nulls, it is also possible that the correspondents might have used nulls for some special miscellaneous purpose, such as for example, to separate an internal message number. Thus, the plain-text message might perhaps look like this:

> REQUEST YOU TRANSMIT ZZZ THREE ZZZ FUNDS IMMEDIATELY

The ZZZ THREE ZZZ might be an internal message number.

Let us somewhat summarize the effects of nulls in the plain-text message. A monoliteral frequency distribution might reveal to the cryptanalyst an abnormal number of a particular low-frequency letter. These low-frequency letters (nulls in the plain-text message) might fall together in the original plain-text. Naturally of course the cryptanalyst must not only be alert to note these abnormal number of low-frequency letters but he must also be able to take advantage of them.

Finally, some remarks should be made concerning specialized plain-text; that is, text which contains words of a specialized nature. A good example might be plain-text which is made up principally of the literal digits, ONE, TWO, THREE, FOUR, FIVE SIX, SEVEN, EIGHT, NINE, and ZERO. Such a plain-text message might be a listing of a group of serial numbers for example. In any case, text of this sort greatly facilitates cryptanalytic solution—provided the cryptanalyst recognizes the situation! Recognizing plain-text of this nature, given only the cipher-text message, is not quite as difficult as at first might be imagined. The monoliteral frequency distribution will show an "uneven" frequency distribution with few if any A's, for example, many E's, N's, and O's, etc. By this time, having recognized the situation, the student should be able quickly to take advantage of known plain-text words.

Another possibility, though admittedly rare, is that where correspondents might mix numbers or digits in with the literal-text. These digits will normally aid solution in that the numbers probably will fall together.

---

[1] This brings out of course the fact that correspondents to get the most out of nulls should use random high-frequency letters.

As a final remark, the student should not overlook the possibility of correspondents either purposely or in error having taken the columns off the enciphering matrix in order from left to right or right to left.

Problems

81. LITIE RWNNW NIEBI EOTEI XRDEO
NSSTN TOEAN ONEAO RIENR WTMES
FHNEG VUTFR HERWF ESZAH TCUEO
EGI

82. PTJTS VAFCS SIHJA NEOJY MPVTE
TOLNI OSITV NOBRJ OEOVM AJCAV
TJUAS

83. YGSLA U2OAA SODNO ENEGS DAEE3
ESM5R ENAEP DR6TS I

84. TEWHR OHIIR OZRIU IFORO NTSOT
EZEFS VTTEO GRLFU WEEEO

85. EEOIN EXNPI HLIIR EOAGF IIOVE
TSUNI SITCI RXFNY AOELB EXRHS
RRZTW OTENN NDMDN ADRWG RBLSA
OMETO SXOSN RPDXU ETSIO OTG

86. RAFAF IQEVD UEEIF NTIEE EEFSO
COFNX IEHER INOVU SEORC ZVZRE
RKRE

87. ALFTO OQIAR TLISV RDFEE EHROR
SETNI RYOIF GQATN QCS

88. ELTHO ISREE ONORX OIAAL CECLS
CPLES IEEGC ATONN SEETX FGTNI
YNUTC NIPPX

89. IE5IE SAOGO HTNOU 9PLLR NS5ES
EGSZS ECRR1 PDEMC YESOX FCO2U
UPITA NSNOD M2LBA

90. SNOAO IUGSE LEOEA TXRXZ VNEER
SORDA EZBWF AXMRZ EEIBE

Chapter XVII

The Computer

In the last two decades the development of the computer as a cryptanalytic tool has substantially enhanced the cryptanalyst's ability to successfully attack many cryptographic systems. While the single columnar transposition cipher has always been considered as a weak system, with the computer at his disposal the cryptanalyst can now make his attack against the cipher even easier.

Against the single columnar transposition cipher the computer generally provides two forms of cryptanalytic assistance:

(1) The computer may be used in matching columns. While this may not be so important when dealing with plaintext, the single columnar transposition cipher may be used to superencipher coded traffic; and in this case the use of a computer to match columns (of coded text) will particularly benefit the cryptanalyst.

(2) The computer can be used in making trial and error tests. Millions of tests can be made quickly and reliably when using state-of-the-art computers plus parallel processing, etc. The trial and error tests, also termed brute-force tests, may involve the complete decipherment of given ciphertext. More often the tests will involve only the "reading" of a certain amount of initial plaintext. If the initial read text turns out to be garbled or random text, the computer will be programmed to drop the test and begin a new test. Of course this is simplification, but the reader has the idea. If the reader is interested in this computer attack against the single columnar transposition cipher, he might consider the problem of identifying plaintext given only a marginal amount of text. At the same time he might consider the number of different numerical keys that can arise from a given key-length. It is evident that the longer the possible key-lengths, the greater becomes the number of trial and error tests required.

For computer-oriented readers the author has written a program in BASICA which provides single columnar transposition enciphermen
The program follows.

```
10 '   (SINGLETR)
20 '   THIS SINGLE COLUMNAR TRANSPOSITION ENCIPHERMENT PROGRAM HAS BEEN
30 '   ESPECIALLY WRITTEN IN "BASICA" FOR THIS TEXT BY WAYNE G. BARKER.
40 CLS
50 CLEAR 1000
60 KEY OFF
70 DEFINT A-Z
80 DIM M1$(1000)
90 DIM W2(1000),D(25),S1(26)
100 DIM A$(50),L$(1000)
110 DIM A(25),T(1000),F$(50,25)
120 DIM W1$(1000),W2$(1000)
130 LPRINT CHR$(27);CHR$(69)
140 INPUT "DO YOU WANT TO ENTER 'NULLS' AT THE END OF MESSAGES (Y OR N)";Q$
150 PRINT
160 IF Q$="n" THEN Q$="N"
170 IF Q$="N" THEN 280
180 IF Q$="Y" THEN 210
190 IF Q$="y" THEN 210
200 GOTO 140
210 INPUT "WHICH LETTER DO YOU WANT TO USE AS A 'NULL'-LETTER";R$
220 PRINT
230 R=ASC(R$)
240 IF R>64 AND R<91 THEN 270
250 IF R>96 AND R<123 THEN R=R-32:GOTO 270
260 GOTO 210
270 R$=CHR$(R)
280 INPUT "Enter Literal Keyword -- ";S$
290 LPRINT
300 FOR I=1 TO LEN(S$)
310 A$(I)=MID$(S$,I,1)
320 A(I)=ASC(MID$(S$,I,1))-64
330 IF A(I)=-32 THEN 370
340 F=F+1
350 IF A(I)>26 THEN A(I)=A(I)-32
360 A(F)=A(I)
370 NEXT
380 LPRINT "Literal Keyword -- ";
390 FOR I=1 TO LEN(S$)
400 LPRINT A$(I);
410 NEXT
420 LPRINT:LPRINT
430 FOR I=1 TO F
440 Z=100
450 FOR J=1 TO F
460 IF A(J)<Z THEN Z=A(J):C=J
470 NEXT
480 A(C)=50
490 D(I)=C
500 NEXT
510 PRINT
520 PRINT "ENTER TEXT"
530 FOR I=1 TO 1000
540 X$=INKEY$
550 IF X$="" THEN LOCATE,,1:GOTO 540
560 IF X$=CHR$(8) THEN Y=Y-1:I=I-2
570 IF X$=CHR$(8) THEN PRINT CHR$(29);
580 IF X$=CHR$(8) THEN PRINT CHR$(255);
590 IF X$=CHR$(8) THEN PRINT CHR$(29);:GOTO 650
600 IF X$=CHR$(13) THEN LOCATE,,0:GOTO 660
```

```
610 PRINT X$;
620 L$(I)=X$
630 M1$(I)=L$(I)
640 Y=Y+1
650 NEXT
660 FOR I=1 TO Y
670 IF ASC(L$(I))>64 AND ASC(L$(I))<91 THEN 720
680 IF ASC(L$(I))>96 AND ASC(L$(I))<123 THEN 700
690 GOTO 750
700 L=ASC(L$(I))-32
710 L$(I)=CHR$(L)
720 X=X+1
730 T=X
740 L$(X)=L$(I)
750 NEXT
760 PRINT:PRINT
770 IF Q$="N" THEN 840
780 Z=INT(5*((X/5)-INT(X/5))+.00001)
790 IF INT(Z)=1 THEN L$(X+1)=R$:L$(X+2)=R$:L$(X+3)=R$:L$(X+4)=R$:U=4
800 IF INT(Z)=2 THEN L$(X+1)=R$:L$(X+2)=R$:L$(X+3)=R$:U=3
810 IF INT(Z)=3 THEN L$(X+1)=R$:L$(X+2)=R$:U=2
820 IF INT(Z)=4 THEN L$(X+1)=R$:U=1
830 T=X+U
840 G=0
850 FOR J=1 TO (INT(T/F)+1)
860 FOR M=1 TO F
870 G=G+1
880 IF G=T+1 THEN 920
890 F$(J,M)=L$(G)
900 NEXT
910 NEXT
920 FOR J=1 TO F
930 B=D(J)
940 FOR M=1 TO INT(T/F)+1
950 V1=V1+1
960 W1$(V1)=F$(M,B)
970 NEXT
980 NEXT
990 U=0
1000 FOR I=1 TO V1
1010 IF W1$(I)="" THEN 1060
1020 U=U+1
1030 W2$(U)=W1$(I)
1040 W2(U)=ASC(W2$(U))-64
1050 S1(W2(U))=S1(W2(U))+1
1060 NEXT
1070 LPRINT
1080 LPRINT "Entered PLAINTEXT message --"
1090 LPRINT
1100 FOR I=1 TO Y
1110 V6=V6+1
1120 LPRINT M1$(I);
1130 IF M1$(I)=CHR$(32) AND V6>60 THEN V6=0:LPRINT
1140 NEXT
1150 LPRINT:LPRINT:LPRINT:LPRINT
1160 LPRINT "Resulting CIPHERTEXT message --"
1170 LPRINT
1180 FOR I=1 TO U
1190 LPRINT W2$(I)" ";
1200 IF I MOD 5=0 THEN LPRINT "  ";
```

```
1210 IF I MOD 25=0 THEN LPRINT
1220 NEXT
1230 LPRINT
1240 LPRINT "("U")"
1250 LPRINT:LPRINT:LPRINT
1260 FOR I=1 TO 26
1270 IF S1(I)=0 THEN LPRINT CHR$(I+64)" = ":GOTO 1290
1280 LPRINT CHR$(I+64)" = "S1(I)
1290 NEXT
1300 LPRINT CHR$(27);CHR$(70)
1310 END
```

Problems

91. NCPEE OOISN YLNEN LXRRE ITRPC
OENSE AIRXT EACTR MEHRH EESDI
ITRNN UUVCF TRDDE LYSTI FFSYU
DQTDI OAOUI KSRUO EFLEA BNSOX
ODOOO OTRRU UHYGP JNIDD EYSAO
EEAAS TMSUE ELWHY EXOCA ETGEX

92. REUOI PKRHT NXEZH PLXNE RUTMA
NNEST HRTDO FOSEI ENRVO UEORU
IEXEY ERTWI DEYQT REOSB XEUTA
OAGOI FEEEO RGRXC QMNOA ITIEI
ZTOOA NEROM SENII UNAGE SESRR
FMNRA PCQEN IZSNT

93. VNDOA RETND EUSRO VTTAB OIOBR
RCNTD EIOGA RULTS HENNI DPDEH
XEOEN HNVME TTRAU TANGT MISCL
EXERE HOBCF ETPYI SAWBY CTRTN
OOXWE CTWSE DHTED NTDPE ROCYS
GLRSA YRARE ERAHA OTAYE EIOHA
OENTX

94. ERRHT OMSHG SHMTT NETLE LOXAX
EIFSO RNSFL OVVEW REPDX CIMEM
LIDYC DORIP EELOE RWVAA NEXNT
YARUA TOETA OHTDT OAEON TGYLR
EEOPU INWTT EHDSI ICTNS XAEES
DMOTD EEOOF UMSLS TIESX

95. SETAE IOHVS PTLES HSGAD FLEAT
LTPLA PBTNH TOTDE TTOFL GUAET
RHLMO ATNIS TTORF NRCAD SEENS
TOITR RALCT TATHE ILFED FPSPA
EOHFT LHTRF OOAIY UTSEN FOPIH
ANOII IAHTA HUOCD OCIRA SESEL
TBEON OTPAW

96. EEIEN OMSQH ATOTT GIELE THDTO
RTOGP AESSX RBTSU HOWET UTSTE
IMTIM GERRR OETDO BENEH HLEAN
ESRPS YSMEM GDXWA NVDUO TUANH
NHINT

97. ETRRA HPOEF TUEEV THDAS NYTNT
ERIAF ALSRI AAADQ ANWRS NBGTR
EZXSE NAYUE TUSNH MBOOT ILEOF
ORURY CIOOC TSGKE EZNZD PSEER
EVNCI TIYAG RLOOA AEVHE TOHEE
EONSO KUIOS ISTQU COEIT EATRT
HUZTI JROAR RIRTD AYLMN OLURP
CNIRT

98. EPUME TTKPP RGOET ASONB SROSE
KSALS TAENE YUHGA ERESC BEPSE
TNPRY SAPNR THUIW ELEOT GIOOO
AANRY

99. PLMMO EAEUM NSCBR NNTXS EDMIP
HKORI ENPAI UTXET EATOY ORULR
AOEKO AXDAE EITMR HONFT TWACR
KWEYO UNNSN GAEIE UEGTA XERNR
NSEBT HIOSS TMAEC

100. RRNRS RENYF ONXFY TUPAO ENSGM
AIIOE OTURE TESLS IOIMS RRCIA
XIIHT AIYEI ESRXY VCQPI CTIED
ATETS TTLTF FPEXR AEEUD PTSVE
DLHSP RMTBE TGLEE SRSEO AIINA

GENERAL INDEX

Adjacent letters,
— definition, 110.
— discussion of, 86-88.
— in enciphering matrix will be separated in final cipher-text message by a multiple of column lengths, 87, 102, 120.
— "limits" of, 107, 109-112, 114, 125.
— "more narrow limits" of, 110-111, 123, 126.
Anagramming, 53-54, 58.
Analytic matrix, 37-43, 46, 79-81, 107, 123.
— "halves", 113-114.
— of completely filled matrix, 53.
— validity of, 114.
— with but one column length, 53.
Art, column matching is an, 59, 114.
"Assists", 117.
"Basic" letter, 87-88, 93-95, 97-99, 110.
Bigraph, 56, 86, 96-97, 100-101, 119-121.
— definition, 24.
— invariable (QU), 99.
— random, 59.
— valid, 59.
— weight of, 55.
Biliteral frequency distribution, 24-30, 44-45, 91-92.
— may serve as monoliteral frequency distribution, 26-28.
Blindness of cryptanalyst, 69.
Brevity, use of "code" to provide, 1.
"Cap" of analytic matrix, 81-83, 113.
Cipher, 1-3.
— combination transposition and substitution systems, 2.
— definition, 1.
— substitution, 1-3.
— systems, 1-3.
— transposition, 1-3.
Cipher-text, 1.
— message, 9, 12-13, 79.
Clear-text message, 14.
Code, 1-3.
— book, 1.
— definition, 1.
— groups, 1, 10.
— systems, 1-2.
Column,
— matching, 52-53, 57-58, 112, 114.
— juxtaposing, 53 (see also *column matching*).
Columns,
— length of, 9, 40-41, 53, 70.
— long, 9, 13-14.
— of analytic matrix compared with columns of enciphering matrix, 41-42.
— short, 9, 13-14.
— taken off enciphering matrix *without* using numerical key, 132.
Completely filled matrix, 52-53, 62-63, 68, 70, 106.
— an impossibility, 130-131.
— definition, 8-9.
Computing,
— column lengths, given key-length and message-length, 12-13, 38, 53, 118.
— size of enciphering matrix, given key-length and message-length, 12-13, 38, 53.
Consonants,
— represented by (c), 124.
— used in column matching, 124-125.

Counting,
— letters in cipher-text message, 12.
— vowels, 64, 113.
Cryptanalyst, 54, 56-57, 62-63, 69, 80, 117, 126, 130-131.
— "good' 'fortune of, 106.
Cryptanalytic difficulty of single columnar transposition cipher, 130.
Cryptanalytic solution,
— given: the plain-text beginning of a message longer than the key-length, 29-34.
— given: plain-text longer than the key-length anywhere in the message, 44-49.
— given: the key-length and a completely filled matrix, 52-59.
— given: the key-length plus a probable word in the text, 79-88.
— given: a probable word in the text, 91-103.
— given: the key-length, 106-114.
— the general solution, 117-127.
Cryptogram, 9, 17, 44, 130.
Cryptographic,
— systems, 1-3.
— text, 10.
Decipherment, 12-16.
— first step, 12, 15.
— second step, 12-13, 15.
— third step, 13-15.
Determination of size of matrix, See *computing*.
Determining factors in solution of single columnar transposition cipher, 130.
Determining length of matrix columns mechanically, 15.
Deviation from the mean, 65.
Difficulty in reading plain-text *without* word divisions, 14-15.
Digits,
— mixed within literal text of transposition cipher, 132.
— phonetically spelled out in the text, See *specialized plain-text.*
— use in substitution ciphers, 1.
— within the numerical key, 4.
Dimensions of matrix, 9, 11-13.
Distance,
— multiple of column lengths, 126.
"Don't give up!"
— advice to the student, 59.
Easily identifiable letters in cipher-text message, 80.
Element necessary to encipher a message, 8, 11.
Enciphered-code, 2.
Enciphering matrix, 8-9, 32, 38, 41, 47-48, 53-54, 58, 86, 103.
Encipherment, 8-11, 15, 52.
— first step, 8, 11, 15.
— second step, 8, 11, 15.
— third step, 9-11, 15.
"Ends" of columns, 83.
Error of correspondents in not using numerical key properly, 132.
Even distribution of vowels in plain-text, 64-68.
Exception to rule,
— reference adjacent letters being separated by a multiple of column lengths in cipher-text message, 87-88.
Expected,
— frequency of English letters in 100 letters of text, 19.
— mean, 65-66, 68.
— percentage of vowels in English text, 21, 23, 28, 64.
— words, 54.
Factors in solution of the single columnar transposition cipher, 130.
Family tree of cryptographic systems, 1-3.
Final remarks, 130-132.

Flow of electricity compared to cryptanalyst's procedure, 117.
Formula to compute percentage of vowels in text, 28.
Foundation for the cryptanalytic solution of columnar transposition cipher systems, 37.
Frequency distribution, 19.
— *norm* (English), 19.
— See also *monoliteral frequency distribution* and *biliteral frequency distribution.*
G, letter occurs in only one of the 100 most frequent trigraphs, 108.
General solution of the single columnar transposition cipher, 106, 117-127.
"Good" bigraphs, such as CK, LY, TH, QU, etc., 53-54, 56, 126.
"Good" trigraphs, 58.
"Good fortune".
— as a factor in solution, 106.
Guessing, 29, 54, 117.
High frequency,
— bigraphs and trigraphs, 69.
— letters used as nulls, 131.
Identification of the "Completely Filled Matrix", 62-69.
Identification of the key-length, 106, 112.
Identification of the transposition cipher,
— through percentage of vowels in message, 21.
— through use of the monoliteral frequency distribution, 19-21.
— through visual inspection, 21-22.
Incomplete square, 8.
Incompletely filled matrix, 52, 62, 106.
— definition, 8, 9.
Insuring that the cryptogram contains all five letter groups, 130.
Internal message number,
— correspondents' use of, 131.
Interpretation of validity values, 65, 67.
Introduction to cryptanalysis of the single columnar transposition cipher, 29-34.
Juxtaposition, 47-49, 53-54, 56-57, 59, 79, 84-86, 96-98, 101-102, 109-112, 119-125.
— definition, 53.
Key, 4-6, 10.
— in a cipher system, 1, 4.
— in a code system, 1.
— literal, 4, 34.
— numerical, 4, 10, 13.
Key-length, 4, 9, 12-13, 32, 37, 46, 68, 70, 79, 106-114, 126-127.
— factor in solution 106.
— not a multiple of five, 130-131.
"Key-Lengths and Column-Lengths of Completely Filled Matrices—Given the Message Length", 62, 70-76.
Key-word, 1, 4, 7, 34.
Least resistance,
— cryptanalyst's desire for path of, 117.
Length of,
— columns, 9, 13-16, 38, 52.
— key, See *key-length.*
— message, See *message-length.*
— time to test a key-length, 106.
Length of message as a factor in solution, 106.
Letter contact weight chart, 55-59, 109.
Letter occurring most frequently in English, 17, 23.
Letter "Q" provides wedge toward solution, 92.
Limitation of possible key-lengths, 106. (See also *restriction by correspondents as to key-lengths.*)

Limits (limitations) of adjacent letters, 81-84, 86-88, 108-109, 122. (See also *adjacent letters.*)
— with two "basic" letters, 110-111, 123.
Literal digits, see *specialized plain-text.*
Literal-key, 4-6.
— recovery not within scope of text, 34.
Literal key-word, 10.
Long column, see *columns.*
Low frequency,
— "good" bigraphs, 126.
— abnormal number of low frequency letters might be "nulls", 131.
Manual determination of matrix size, 15.
Marking off of columns within message (analytic matrix), 81-83.
Matching, (See also *juxtaposition.*)
— low frequency letters, 119.
— segments, 126.
Matrix,
— completely filled, 8-9, 52-53, 106, 130-131.
— definition, 8.
— in-completely filled, 8-9, 52-53, 106, 131.
— see also *analytic matrix* and *enciphering matrix.*
— size expressed by column lengths, 38.
— size of, see *computing.*
Mean difference, 65-66, 68.
Mechanical,
— column matching is not, 59.
— construction of analytic matrix, 79.
— method of determining length of matrix columns, 15.
Memorization,
— difficulty in memorizing numerical key, 4.
Message length, 9, 13, 15, 38, 53, 63, 70, 130.
Monoliteral frequency distribution, 17-22, 24, 79-80, 107, 118, 131.
— definition, 17.
Multiple of five as key-length, 130.
"Narrow" limits of adjacent letters, see *adjacent letters.*
Norm for English text, 19-20.
Nulls, 130-131.
— definition, 130.
— used to separate internal message number, 131.
Number of,
— long columns, 13, 16, 38.
— short columns, 13, 16, 38.
Numerical-key, 4, 8, 10, 12, 34, 48.
— how to derive from literal-key, 4-6.
— same numerical-key may result from two different literal-keys, 5-6.
"Odds and ends", 130.
Percentage of column lengths which *cannot* have resulted from a completely filled matrix, 63.
Physical determination of size of matrix, 15.
Plain-text,
— as a factor in solution, 106, 130.
— message, 14-15, 58, see also *clear-text message.*
— see also *specialized plain-text.*
— treatment in cipher system, 1, 3.
Probable word,
— in the text, 79-80, 84, 87, 91-72, 16, 117.
— method, 127.
Problems to be solved by student, 35-36, 50-51, 60-61, 77-78, 81-90, 104-105, 115-116, 128-129, 133-134.

Procedure for determining whether or not given column lengths will fit into a given distance, 120.
Q,
— importance of letter, 92.
— invariably followed by letter U, 21, 23, 53, 69, 93, 99-100.
QU, invariably followed by a vowel, 100.
Questions to be answered by student, 3, 7, 11, 16, 23, 28, 43.
Quotient, 120.
Random,
— bigraph, 59.
— numerical-keys, 7.
— high-frequency letters and their use, 131.
Rearranging columns, see *juxtaposition.*
Recovery of the literal-key is not within scope of text, 34.
Reliability of validity values, 64-65.
Restriction by correspondents as to key-lengths, 130-131.
"Science", column matching is not a, 59, 114.
Secret inks, 2.
Security, use of "code" to provide, 1.
Segments of cipher-text, 121, 126.
Short column, see *columns.*
Short form, for expressing matrix size, 38, 103.
Single columnar transposition cipher,
— text covers completely, 130.
— where it fits in the family tree of cryptographic systems, 2.
Size of matrix, 9, 12, 15, 62, see also *matrix* and *computing.*
Sizes of completely filled matrices, 70-76.
Specialized plain-text, 131-132.
Steps,
— in decipherment, 12-16.
— in encipherment, 8-11, 15.
Stereotype, 29.
Substitution cipher, 1-2.
Successive letters, separated in the final cipher-text by a multiple of of column lengths, 87.
Summarization of the general solutions, 126.
Superfluous letters, 41, 48.
Symbols used in substitution cipher systems, 1.
Table,
— of key-lengths and column-lengths of completely filled matrices— given the message-length, 70-76.
— of the 100 most frequent trigraphs, 108.
— of the expected frequency of letters in English, 19.
Testing for completely filled matrix, 63.
Theory,
— behind test with respect to incompletely filled matrices, 112-114.
— behind the limitations within columns, 86-88.
Tools of the cryptanalyst, 37, 62, 114.
Traffic, 34.
Transposition cipher, 1-3, 19, 28.
Trial-and-error, 29, 91, 117, 127.
Trigraph, 58, 121, 124.
Trigraphs, 100 most frequent, 108.
"Troughs and peaks", used in comparing frequency distributions, 20.
"Uneven" frequency distribution, 132.
Valid,
— analytic matrix, 64, 69, 113-114.
— bigraph, 59.
— matrix, 67.
Validity value of the matrix, 65-69.
— reliability of, 64-66.
Validity weight, 56, 109-110.

— reliability of, 59.
Visually matching columns, 57, 114.
Vowels,
— evenly distributed in text, 64, 67, 112.
— expected percentage in English text, 21, 23, 28, 64.
— represented by (v), 124.
— which letters constitute, 21.
— will follow the bigraph QU, 100.
— will precede certain combinations of letters, 121.
Words, anagramming of, 54.

BOOKS IN THE CRYPTOGRAPHIC SERIES

---

1 – **Manual for the Solution of Military Ciphers**, Parker Hitt
2 – **Cryptanalysis of the Simple Substitution Cipher with Word Divisions**, Wayne G. Barker
3 – **Elements of Cryptanalysis**, William F. Friedman
4 – **Statistical Methods in Cryptanalysis**, Solomon Kullback, Ph.D.
5 – **Cryptography and Cryptanalysis Articles, Vol. 1**, edited by W.F. Friedman
– **Cryptography and Cryptanalysis Articles, Vol. 2**, edited by W.F. Friedman
9 – **War Secrets in the Ether, Vol. 1**, Wilhelm F. Flicke
– **War Secrets in the Ether, Vol. 2**, Wilhelm F. Flicke
13 – **The Zimmerman Telegram of January 16, 1917, and its Cryptographic Background**, William F. Friedman & Charles J. Mendelsohn, Ph.D.
17 – **Cryptanalysis of the Hagelin Cryptograph**, Wayne G. Barker
18 – **The Contributions of the Cryptographic Bureaus in the World War** [World War I], Yves Gylden
20 – **History of Codes and Ciphers in the U.S. Prior to World War I**, ed. Wayne G. Barker
21 – **History of Codes and Ciphers in the U.S. During World War I**, ed. Wayne G. Barker
22 – **History of Codes and Ciphers in the U.S. During the Period Between the World Wars, Part I. 1919-1929**, ed. Wayne G. Barker
30 – **Military Cryptanalysis, Part I**, William F. Friedman
35 – **The Origin and Development of the National Security Agency**, George A. Brownell
36 – **Treatise on Cryptography**, Andre Lange and E.A. Soudart
39 – **Cryptanalysis of Shift-Register Generated Stream Cipher Systems**, Wayne G. Barker
40 – **Military Cryptanalysis, Part II**, William F. Friedman
41 – **Elementary Course in Probability for the Cryptanalyst**, [Rev. Ed.], Andrew M. Gleason
42 – **Military Cryptanalytics, Part I, Vol. 1**, W.F. Friedman and L.D. Callimahos
43 – **Military Cryptanalytics, Part I, Vol. 2**, W.F. Friedman and L.D. Callimahos
44 – **Military Cryptanalytics, Part II, Vol. 1**, L.D. Callimahos and W.F. Friedman
45 – **Military Cryptanalytics, Part II, Vol. 2**, L.D. Callimahos and W.F. Friedman
46 – **Pattern Words: Three Letters to Eight Letters in Length**, Sheila Carlisle
47 – **Cryptology and the Personal Computer with Programming in Basic**, Karl Andreassen
48 – **Pattern Words: Nine Letters in Length**, Sheila Carlisle
49 – **The Index of Coincidence and its Applications in Cryptanalysis**, [illegible] F. Friedman
50 – **Cryptographic Significance of the Knapsack Problem**, Lu[illegible] Connor a[illegible] Seber[illegible]
52 – **The American Black Chamber**, Herbert O. Yardley
53 – **Traffic Analysis and the Zendian Problem**, L.D. Call[illegible]
54 – **History of Codes and Ciphers in the U.S. During the Period Between the World Wa[illegible] Part II, 1930-1939**, ed. Wayne G. Barker
55 – **Introduction to the Analysis of the Data Encryption** [illegible]
56 – **Elementary Cryptography and Cryptanalysis**, Donald D. M[illegible]
57 – **Secret Ciphers of the 1876 Presidential Election**, D. Beaird [illegible]

AEGEAN PARK PRESS, P.O. Box 2837, Laguna Hill[illegible]

מכללת אורט בראודה
הספרים
23694-10
Cryptanalysis of the single